

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

HEARINGS

BEFORE THE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES,
AND THE ADMINISTRATION OF JUSTICE

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

FIRST AND SECOND SESSIONS

ON

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

NOVEMBER 2, 3, 1983, AND JANUARY 24, APRIL 5, AND SEPTEMBER 26,
1984

Serial No. 103



Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

WASHINGTON : 1984

COMMITTEE ON THE JUDICIARY

PETER W. RODINO, JR., New Jersey, *Chairman*

JACK BROOKS, Texas	HAMILTON FISH, JR., New York
ROBERT W. KASTENMEIER, Wisconsin	CARLOS J. MOORHEAD, California
DON EDWARDS, California	HENRY J. HYDE, Illinois
JOHN CONYERS, JR., Michigan	THOMAS N. KINDNESS, Ohio
JOHN F. SEIBERLING, Ohio	HAROLD S. SAWYER, Michigan
ROMANO L. MAZZOLI, Kentucky	DAN LUNGREN, California
WILLIAM J. HUGHES, New Jersey	F. JAMES SENSENBRENNER, JR., Wisconsin
SAM B. HALL, JR., Texas	BILL McCOLLUM, Florida
MIKE SYNAR, Oklahoma	E. CLAY SHAW, JR., Florida
PATRICIA SCHROEDER, Colorado	GEORGE W. GEKAS, Pennsylvania
DAN GLICKMAN, Kansas	MICHAEL DeWINE, Ohio
HAROLD WASHINGTON, Illinois	
BARNEY FRANK, Massachusetts	
GEO. W. CROCKETT, JR., Michigan	
CHARLES E. SCHUMER, New York	
BRUCE A. MORRISON, Connecticut	
EDWARD F. FEIGHAN, Ohio	
LAWRENCE J. SMITH, Florida	
HOWARD L. BERMAN, California	

ALAN A. PARKER, *General Counsel*

GARNEE J. CLINE, *Staff Director*

ALAN F. COFFEY, JR., *Associate Counsel*

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES, AND THE ADMINISTRATION OF JUSTICE

ROBERT W. KASTENMEIER, Wisconsin, *Chairman*

JACK BROOKS, Texas	CARLOS J. MOORHEAD, California
ROMANO L. MAZZOLI, Kentucky	HENRY J. HYDE, Illinois
MIKE SYNAR, Oklahoma	MICHAEL DeWINE, Ohio
PATRICIA SCHROEDER, Colorado	THOMAS N. KINDNESS, Ohio
DAN GLICKMAN, Kansas	HAROLD S. SAWYER, Michigan
BARNEY FRANK, Massachusetts	
BRUCE A. MORRISON, Connecticut	
HOWARD L. BERMAN, California	

MICHAEL J. REMINGTON, *Chief Counsel*

GAIL HIGGINS FOCARTY, *Counsel*

DAVID W. BEIER, *Counsel*

DEBORAH LEAVY, *Counsel*

THOMAS MOONEY, *Associate Counsel*

JOSEPH V. WOLFE, *Associate Counsel*

CONTENTS

HEARINGS HELD

	Page
November 2, 1983.....	1
November 3, 1983.....	49
January 24, 1984.....	133
April 5, 1984.....	259
September 26, 1984.....	331

WITNESSES

Abrams, Floyd, attorney, Cahill, Gordon and Reindel	3
Prepared statement	6
Bamford, James, author of "The Puzzle Place".....	36
Prepared statement	38
Bok, Sissela, professor, Harvard University.....	246
Prepared statement	251
Brinkley, David, senior correspondent, ABC News.....	13
Prepared statement	14
Carr, James, U.S. magistrate.....	146
Chancellor, John, senior commentator, NBS News	12
Prepared statement	12
Davida, George I., professor, Department of Electrical Engineering and Computer Science.....	90
Prepared statement	93
Goldsmith, Michael, professor of law Vanderbilt Law School	151
Prepared statement	158
Hoffman, Alexander C., chairman, Direct Marketing Association Inc	308
Prepared statement	311
Joyce, Edward, president, CBS News.....	9
Prepared statement	11
Laudon, Kenneth C., professor, of Computer Applications.....	296
Prepared statement	304
Lawton, Esq., Mary C., Director, Office of Intelligence Policy and Review, Department of Justice.....	366
Prepared statement	371
Magrath, Peter C., president of the University of Minnesota.....	59
Prepared statement	51
McGehee, Ralph W., former CIA agent, author of "Deadly Deceits"	41
Prepared statement	44
Oettinger, Anthony G., chairman, Information Policy Research, Harvard University.....	229
Prepared statement	233
Plessler, Esq., Ronald L., Blum, Nash & Railsback, Washington, DC	349
Prepared statement	354
Press, Frank, president, National Academy of Sciences	63
Prepared statement	68
Schwartz, Herman, professor of law, American University	134
Prepared statement	139
Shattuck, Esq., John, vice president for government, Community and Public Affairs for Harvard University	333
Prepared statement	339
Smith, Robert E., publisher, Privacy Journal	260
Prepared statement	267
Trabow, George B., professor, the John Marshall Law School	322
Prepared statement	326

IV

	Page
Unger, Stephen H., professor, Computer Science Department	118
Prepared statement	123
Ware, Willis H., corporate research staff, Rand Corp	218
Prepared statement	222
Willenbrock, Karl F., chairmah, IEEE Technology Transfer Committee	99
Prepared statement	105

ADDITIONAL MATERIAL

Committee insert, essay, Up Against Them	23
------------------------------------------------	----

APPENDIXES

APPENDIX I

APPENDIX I—MISCELLANEOUS ARTICLES

Cronkite, "Orwell's '1984'—Nearing?," New York Times, June 5, 1983	393
Abrams, "The New Effort to Control Information," New York Times Magazine, September 25, 1983	394
Shattuck, "National Security a Decade After Watergate," Democracy (Winter, 1983)	401
Emerson, "The State of the First Amendment as We Enter '1984,'" Yale L. Rep. 15 (Spring, 1984)	417

APPENDIX II—MATERIALS RELATING TO RESTRICTIONS ON THE PRESS IN GRENADA

House Resolution 384, 98th Cong. 1st Sess. (1983)	425
News Release by the Secretary of Defense dated August 23, 1984, and attached Final Report of the CJCS Media Military Relations Panel (Sidle Panel)	427
Humphries, "Two Routes to the Wrong Destination: Public Affairs in the South Atlantic War," 36 Naval War C. Rev. 57 (No. 3) (1983)	447
Gottschalk, "Consistent with Security" . . . A History of American Military Press Censorship," 5 Comm. and the Law 35 (1983)	463
"U.S. Troops Remove Four Reporters," Washington Post, October 27, 1983	481
"Invasion Secrecy Creating a Furor: Speakes Complained in Memo," Washington Post, October 27, 1983	482
"Administration Limits News of Grenada," New York Times, October 27, 1983	484
"U.S. Forces Thwart Journalists' Reports," Washington Post, October 28, 1983	485
"Censoring the Invasion," Washington Post, October 28, 1983	486
McCloskey, "Invasion and Evasion," Washington Post, October 28, 1983	486
"U.S. 'News Control' on Grenada," Washington Post, October 28, 1983	487
"In Barbados, a Restless Press," Washington Post, October 29, 1983	488
"Information Out of Sync," Washington Post, October 29, 1983	489
Lewis, "What Was He Hiding?," New York Times, October 31, 1983	490
"Admiral Fights 2 Battles: With Grenada and Press," Washington Post, October 31, 1983	491
Grunwald, "Trying to Censor Reality," Time, November 7, 1983	494
"U.S. Press Curbs in Grenada May Affect International Debate," New York Times, November 8, 1983	495
Cohen, "Hey!," Washington Post, November 13, 1983	496
"Information Blackout Revives Old Issues," Washington Post, November 15, 1983	497
Cartoon by Herblock, Washington Post, November 16, 1983	499
"Shultz Defends Press Ban," Washington Post, December 16, 1983	500
Johnson, "Echoes," Washington Post, January 29, 1984 (results of Harris Poll on the press in Grenada)	501
Middleton, "Barring Reporters From the Battlefield," New York Times Magazine, February 5, 1984	502
"U.S. Bars Reporters From Naval Exercises," Washington Post, May 6, 1984	506
"Pentagon Plans Media Pool to Cover Missions," Washington Post, August 24, 1984	507

	Page
"Pentagon Forms War Press Pool: Newspaper Reporters Excluded," New York Times, October 11, 1984.....	508
Letter to House Committee on the Judiciary from Thomas J. Roche, Jr., dated November 4, 1983.....	510
Letter to Hon. Robert W. Kastenmeier from John Hendry dated October 30, 1983.....	511
Letter to Hon. Robert W. Kastenmeier from Ralph D. Bradway dated November 8, 1983.....	512
Letter to Hon. Robert W. Kastenmeier from Elbert N. Mullis, Jr., dated November 4, 1983.....	514
Letter to David Brinkley from S.H. Byers, President, Byco, Inc., dated November 4, 1983.....	515

APPENDIX III—PREPUBLICATION REVIEW PRACTICES BY GOVERNMENT AGENCIES

Barnford, "How I Got the N.S.A. Files: How Reagan Tried to Get Them Back," Nation, November 6, 1982.....	516
Memorandum from William French Smith, Attorney General, to heads of offices, boards, divisions and bureaus, dated March 11, 1983, regarding Presidential Directive on Safeguarding National Security Information.....	519
Burnham, "The Silent Power of the N.S.A.," New York Times Magazine, March 27, 1983.....	526
Letter to Hon. Glenn English from Lincoln D. Faurer, Director, N.S.A., dated June 14, 1983. Attachment: Responses to questions from Representative Glenn English.....	532
Letter to Hon. Robert W. Kastenmeier from Don Sellar, Prairie Correspondent, Southam News of Canada, dated October 28, 1983. Attachments: "FBI Quizzes Canadian Correspondent About Source of Defense Information," the Washington Post, September 1, 1983. Arvidson, "The FBI Bears Down," Columbia Journalism Review, September/October 1983.....	541
Taubman, "Security Agency Bars Access to Nonsecret Material, Library Records Show," New York Times, April 28, 1984.....	546
R. McGehee, Deadly Deceits 196-203 (Appendix: This Book and the Secrecy Agreement).....	548

APPENDIX 2

APPENDIX I—MISCELLANEOUS MATERIALS

Letter from Professor George I. Davida, University of Wisconsin—Milwaukee, to Hon. Robert W. Kastenmeier, dated October 28, 1983. Attachment: "American Council on Education, Report of the Public Cryptography Study Group," February 7, 1981.....	557
Letter from Jonathan Knight, Associate Secretary, American Association of University Professors, to David Beier, Esq., Counsel, House Committee on the Judiciary, dated October 31, 1983. Attachment: "American Association of University Professors, Government Censorship and Academic Freedom"....	583
"American Association for the Advancement of Science, Project on Secrecy and Openness in Scientific and Technical Communication," October 1983.....	595
Letter from William D. Carey, Executive Officer, American Association for the Advancement of Science, to Hon. Robert Kastenmeier, dated February 15, 1984.....	598
Letter from A. Bartlett Giamatti, President, Yale University, to Hon. Robert Kastenmeier, dated December 12, 1983.....	601

APPENDIX II—ARTICLES AND PAPERS

"American Civil Liberties Union, Free Speech, 1984: The Rise of Government Controls on Information, Debate and Association," July 1983.....	602
Relyea, "Shrouding the Endless Frontier—Scientific Communications and National Security: Considerations for a Policy Balance Sheet," 1 Gov't. Information Q. 1 (1984).....	631
Gelbspan, "U.S. Tightening Access to Information" (3-part series), Boston Globe, January 22, 23, 24, 1984.....	646
Ehlke & Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," 30 Fed. Bar News & J. 91 (1983).....	652

	Page
"American Association for the Advancement of Science, Scientific Freedom and National Security," June 1984.....	660
"Federal Restrictions on Research: Academic Freedom and National Security," <i>Academe</i> , September/October 1982 at 19.....	668
Gray, "Technology Transfer at Issue: The Academic Viewpoint," <i>IEEE Spectrum</i> , May 1982, at 64.....	671
Wallich, "Technology Transfer at Issue: The Industry Viewpoint," <i>IEEE Spectrum</i> , May 1982, at 69.....	676
Pyle, <i>The Invasion of Privacy</i> , 34 <i>Proc. of the Acad. of Pol. Sci.</i> 131 (1982).....	682
Kamen, "Appeals Court Upholds CIA Censorship of Article," <i>Washington Post</i> , October 5, 1983.....	694
"National Security and Scientific Freedom," <i>AAAS Committee on Scientific Freedom and Responsibility Bulletin</i> , September 1982.....	695
Massachusetts Institute of Technology, <i>Interim Report of the Committee on the Changing Nature of Information</i> , March 9, 1983.....	698
Unger, "The Growing Threat of Government Secrecy," <i>Technology Review</i> , February/March 1982 at 31.....	706
R. Park, <i>Scientific Freedom: Where Does Congress Stand?</i> (unpublished paper).....	717
Chalk, "Commentary on the NAS Report," 8 <i>Science, Technology, & Human Values</i> 21 (1983).....	728
Rosenbaum, Tenzer, Unger, Van Alstyne & Knight, "Academic Freedom and the Classified Information System," 219 <i>Science</i> 257 (1983).....	734
American Association for the Advancement of Science, <i>Committee on Scientific Freedom and Responsibility, National Security and Scientific Communication</i> (June 1982).....	737
W.D. Cooke, T. Eisner, T. Everhart, F. Long, D. Nelkin, B. Windom, E. Wolf, <i>Restrictions on Academic Research and the National Interest</i> (unpublished paper).....	749
Ferguson, "Scientific Freedom, National Security, and the First Amendment," 221 <i>Science</i> 620 (1983).....	769
Ferguson, "Scientific and Technological Expression: A Problem in First Amendment Theory," 16 <i>Harv. C.R.-C.L. L. Rev.</i> 519 (1981).....	775
Corson, "What Price Security?," <i>Physics Today</i> , February 1983, at 42.....	817
Pike, "When Science is Outlawed," <i>Inquiry</i> , March 29, 1982, at 21.....	822
Harvard University, <i>Federal Restrictions on the Free Flow of Academic Information and Ideas</i> , January 1985.....	827

APPENDIX 3

APPENDIX I—ARTICLES

Soma & Wehmhoefer, "A Legal and Technical Assessment of the Effect of Computers on Privacy," 60:3 <i>Den L.J.</i> 449 (1983).....	862
"The High-Tech Threat to Your Privacy," <i>Changing Times</i> , April 1983, at 61.....	897
Dubro, "Your Medical Records. How Private Are They?" <i>California Lawyer</i> , April 1983, at 33.....	900
Neustadt & Swanson, "Privacy and Videotex Systems," <i>Byte</i> , July 1983 at 98.....	903
Smith, "Probing the Capitol's Drug Store," 9 <i>Privacy Journal</i> , September 1983.....	905
Attachment: Advertisement for Computerized Prescription System at Giant Pharmacies.....	906
Boorman & Levitt, "Big Brother and Block Modeling," <i>New York Times</i> , November 20, 1983.....	907
Boorman & Levitt, "Block Models and Self-Defense," <i>New York Times</i> , November 27, 1983.....	908
Rule, McAdam, Stearns, & Uglow, "Documentary Identification and Mass Surveillance in the United States," <i>Social Problems</i> , December 1983, at 222.....	910
Clymer, "Privacy Threats Worry Americans," <i>New York Times</i> , December 8, 1983.....	923
Burnham, "IRS Starts Hunt for Tax Evaders, Using Mail-Order Concerns' Lists," <i>New York Times</i> , December 25, 1983.....	923
Brownstein, "Computer Communications Vulnerable as Privacy Law Lag Behind Technology," 16 <i>National Journal</i> 52 (1984).....	926
Burnham, "IRS Seeks Links to County Computers in Texas to Find Debtors," <i>New York Times</i> , March 13, 1984.....	932
Burnham, "U.S. Agencies to Get Direct Link to Credit Records," <i>New York Times</i> , April 8, 1984.....	933

VII

	Page
Grier, "Who's Snooping and How? U.S. and U.S.S.R. 'Peer Into Mist'," (pts. 2-6), <i>Christian Science Monitor</i> (April 17, 18, 19, 20, 23, 1984).....	934
Earley, "Government to Share Deadbeat, List With Private Credit-Rating Bureaus," <i>Washington Post</i> , April 25, 1985.....	943
Shattuck, "Computer Matching is a Serious Threat to Individual Rights," 27 <i>Communications of the ACM</i> 538 (June 1984).....	945
Burnham, "IRS Rejected in Hunt for Estimated Income Lists," <i>New York Times</i> , October 31, 1984.....	949
University of Maryland, Center for Philosophy and Public Policy, "Privacy in the Computer Age," <i>QQ</i> , Fall 1984.....	951

APPENDIX II—MISCELLANEOUS MATERIAL

The Direct Mail/Marketing Association's "Suggested Guidelines for Personal Information Protection" (1982).....	957
National Defense University, Department of Defense Computer Institute, "Selected Computer Articles 1983-84".....	963
Yudovich, "Administrative Surveillance—A Means of Police Repression," December 6, 1983 (translation prepared by Radio Liberty Research (RL-454/83)).....	967
Marx & Reichman, "Routinizing the Discovery of Secrets," 27 <i>American Behavioral Scientist</i> , March/April 1984, at 423.....	972
Letter to Hon. Robert W. Kastenmeier from Robert A. McConnell, Assistant Attorney General, U.S. Department of Justice, dated March 30, 1984.....	1002

APPENDIX 4

APPENDIX I—LEGISLATIVE MATERIALS

H.R. 6343, 98th Cong., 2d Sess. (1984).....	1006
---------------------------------------------	------

APPENDIX II—CASES

<i>U.S. v. Truong Dinh Hung</i> , 629 F.2d 908 (4th Cir. 1980).....	1015
<i>U.S. v. Seidlitz</i> , 589 F.2d 152 (4th Cir. 1980).....	1017
<i>U.S. v. Butenko</i> , 494 F.2d 593 (3d Cir. 1974).....	1026
<i>People v. Teicher</i> , 52 N.Y. 2d 638 (Ct. of Appeals, 1981).....	1048
<i>People v. Teicher</i> , 395 N.Y.S. 2d 587 (Sup. Ct. 1977).....	1059
<i>State v. Jennings</i> , 611 P.2d 1050 (Idaho, 1980).....	1073
<i>U.S. v. New York Telephone Co.</i> , 434 U.S. 159 (1977).....	1080
<i>Simmons v. Southwestern Bell Telephone Co.</i> , 452 F. Supp. 392 (W.D. Okla. 1978).....	1113
<i>U.S. v. Hall</i> , 488 F.2d 193 (1973).....	1119
<i>Smith v. Wunker</i> , 356 F. Supp. 44 (S.D. Ohio 1972).....	1128
<i>Jabara v. Webster</i> , — F.2d — (6th Cir. 1984).....	1132
<i>State of Kansas v. Howard</i> , — Kan. — (Kan. Sup. Ct. 1983).....	1146
<i>People v. Dezek</i> , Mich. App., 308 N.W.2d 652 (1981).....	1167
"Application of Order Authorizing Interception of Oral Communications and Videotape Surveillance", 513 F. Supp. 421 (1980).....	1175
<i>U.S. v. Torres</i> , — F.2d — (7th Cir. 1984).....	1178
<i>U.S. v. Bowler</i> , 561 F.2d 1323 (1977).....	1217

APPENDIX III—ARTICLES AND MISCELLANEOUS MATERIALS

Burnham, "Can Privacy and Computer Coexist?," <i>New York Times</i> , November 5, 1983.....	1221
Brownstein, "Computer Communications Vulnerable as Privacy Laws Lag Behind Technology," 16-2 <i>Nat'l Journal</i> 52 (January 14, 1984).....	1222
Globe, "Spy Tech," <i>Christian Science Monitor</i> (pts. 1-6) April 16, 17, 18, 19, 20, and 23, 1984.....	1228
Schrage, "U.S. May Tighten Electronic Net to Control Software," <i>Washington Post</i> , May 6, 1984.....	1242
Burnham, "Reagan Orders Action on Eavesdropping," <i>New York Times</i> , October 15, 1984.....	1244
Serrill, "The No Man's Land of High Tech," <i>Time</i> , January 14, 1985.....	1245
Letter from U.S. Department of Justice, Criminal Division, to Hon. Robert W. Kastenmeier, dated December 27, 1983, with attachments.....	1246

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

WEDNESDAY, NOVEMBER 2, 1983

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met at 9:30 a.m. in room 2141 of the Rayburn House Office Building; the Honorable Robert M. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Mazzoli, Synar, Schroeder, Glickman, Morrison, Moorhead, Hyde, DeWine, Kindness, and Sawyer.

Staff present: Deborah Leavy, David W. Beier, counsel; Joseph V. Wolfe, associate counsel; Audrey Marcus, clerk.

Mr. KASTENMEIER. The committee will come to order.

Mr. SYNAR. Mr. Chairman.

Mr. KASTENMEIER. The gentleman from Oklahoma.

Mr. SYNAR. Mr. Chairman, I move the committee permit the meeting this morning to be covered, in whole or in part, by television broadcast, radio broadcast and/or still photography, pursuant to rule 5 of the committee rules.

Mr. KASTENMEIER. Without objection, the motion is agreed to.

The Chair will state that some of our members are in party caucus and will be here momentarily. Prior to hearing any formal opening statement, I would like this opportunity to put our hearing in an institutional and historical context.

Throughout our Nation's history there has been tension between the first amendment and other governmental interests. Resolution of these competing needs has been a difficult and often stormy process. Frequently, we think in terms of these many conflicts being resolved by the Federal courts. As vital as preservation of that forum is for all of us, the courts are not the only place for dealing with these issues.

As Holmes said several decades ago, "It must be remembered that legislatures are the ultimate guardians of the liberties and welfare of the people in quite the same degree as the courts."

Those of us fortunate to serve in an elected capacity in Congress or elsewhere have a special responsibility to uphold the Constitution. In the past decade this committee, indeed, this subcommittee, has been involved in more than one of these disputes. My col-

leagues and I joined together in a bipartisan effort to respond to the Supreme Court decision in *Stanford Daily v. Zurcher*.

We have undertaken similar initiatives dealing with reporter's privilege, privacy protection from intrusive wiretapping in terms of domestic law enforcement, to the passage of the bill on the Foreign Intelligence Surveillance Act, and even prior to that, to ridding ourselves of title II of the Internal Security Act, wherein this Nation maintained detention camps similar to those that were utilized at the outset of World War II.

I recite this history to establish that these hearings are part of an historical continuum. The issues we will address today are not partisan in nature. They are part of a diligent oversight of the executive branch.

We begin the first of 2 days of the series of hearings on "1984: Civil Liberties and the National Security State." Since George Orwell penned his famous novel of life under "Big Brother," the year 1984 has had an ominous sound, threatening to ring in an era in which civil liberties would be crushed under the heels of the State.

The very fact that we hold these hearings today is solid evidence that such a world has not yet arrived. But Orwell's "1984" was not intended to be a promise or even a prediction. It was a warning. The coming of the year 1984 thus offers a unique opportunity to examine the state of our civil liberties as well as what the future may hold in the light of Orwell's fears and our own.

Among the most important themes developed by Orwell is the justification used by the State for the development of both secret surveillance over activity of its citizens and control over information through the "Ministry of Truth."

In "1984" the rationale for repression was the existence of total war. In our era, it may well be the creation in the last quarter of the century of a new culture, a national security culture protected from the influences of American life by the shield of secrecy.

The evolution of national security as the predominant concern of the Federal Government appears to have been influenced by both increased international tensions and shifts in ideology.

In the years that immediately followed the Second World War, concerns over national security produced statutes that reduced the flow of information: the Atomic Energy Act, the Patent Secrecy Act, the McCarran Act. These were enacted at a time when a heightened sense of conflict in foreign affairs coincided with the rise of McCarthyism.

As the Nation passed through the cold war phase, the country's laws and information practices gradually changed in the other direction. Congress enacted measures aimed at privacy: the Privacy Act, the Bank Records Secrecy Act, the Foreign Intelligence Surveillance Act, title III of the Omnibus Crime Control Act on wiretapping, as well as statutory safeguards on the free flow of information.

In recent years, however, the pendulum has begun again to swing back toward restrictions on civil liberties, as witnesses will develop more fully in their testimony today and in the hearings to come.

I would like at this point to introduce our opening witness. There is no finer first amendment lawyer than Floyd Abrams. A graduate of Yale Law School, he is a partner in the New York City firm of Cahill, Gordon & Reindel. Mr. Abrams has considered the conflict between national security and the free flow of information as an attorney on cases such as the *Pentagon Papers* case, and is the author of the lead article in the New York Times Sunday magazine which featured him on the same issue.

We are very pleased to have you here this morning, Mr. Abrams. You may proceed as you wish.

TESTIMONY OF FLOYD ABRAMS, ATTORNEY, CAHILL, GORDON & REINDEL.

Mr. ABRAMS. Chairman Kastenmeier and members of the subcommittee, I am honored by your invitation to testify today. Apart from my pleasure about being here, I do admire your choice of topic.

Mr. KASTENMEIER. Please see if the microphone is working.

Mr. ABRAMS. Is the mike on?

Thank you; I was saying, Congressman Kastenmeier, that I admire your choice of topics for these hearings this morning. It seems to me that you have chosen a central one for the future of our country. And as we meet virtually on the eve of 1984, the Orwellian nightmare referred to by you, lucid as it is, offers us a basis for learning and for comparison.

Allow me at that outset to recall for you Orwell's grim vision of 1984 as set forth in his book. It is of a nation, Oceania, of which we and Great Britain are a part, which is perpetually at war with the other two superpowers of the world. It is of a society premised on terror, totally dominated by totalitarian rulers, in which any who differ are bludgeoned by their rulers, brainwashed and ultimately either vaporized or, as the hero in the book, himself utterly drained of humanity and filled with only those thoughts that the State chooses that he have.

If you want a picture of the future, Winston Smith, the hero of the book is told by the individual who is involved in the torture of him, imagine a boot stamping on a human face forever.

"1984" is also a vision of the State with the clearest possible views of the dangers of truth, a State which has not only redefined falsehood as truth but in which the definition of truth constantly changed, a society in which the hero finds an old newspaper clipping conclusively proving that the confessions of three supposed traitors were fraudulent, that they were in fact not at the place they had confessed to being at, and which he then thinks the following to himself: "There was only one possible conclusion: the confessions were lies."

Of course, this is not in itself a discovery. Even at that time Winston had not imagined that the people who were wiped out in the purges had actually committed the crimes that they were accused of. But this was concrete evidence; it was like a fragment of the abolished past, like a fossil bone which turns up in the wrong stratum and destroys a geological theory. It was enough to blow the

party to atoms, if in some way it could have been published to the world and its significance made known.

Of course, it was never published to the world, and the hero himself is later bludgeoned, tortured, and brainwashed into believing that he had never seen the clipping, that it had, indeed, never existed.

It is, of course, not our society. It is worth saying that today. It will not be our society in 1984. Or, we may hope, thereafter.

It is worth pausing for a moment on why that is so. In good part, it is because we live under a system of law with a Bill of Rights which protects against just the elements of "1984" we find most offensive—in short, a State that directs us, controls us and ultimately rules us. We are, need I say, not tortured because we hold different views than our Government.

In fact, so far does our constitutional protection go that truthful statements are almost totally insulated from Government sanctions of any sort. So far does our protection go that we are free to express any opinion without fear of governmentally imposed sanctions. There is no such thing in this country, Justice Lewis Powell has said for the U.S. Supreme Court, "as a false opinion."

Our law, then, goes far toward protecting us against the "1984" nightmare becoming a reality. The absence of such legal protection is evident abroad. Consider one portion of the public interrogation at the trial of Soviet dissident Sinyavsky, a portion which—fittingly—could be annexed to an updated version of "1984." Accused of anti-Soviet behavior, the prosecutor asked this great author the following: Prosecutor, "Please don't lecture us on literature. I asked you one simple, concrete question: Why did you portray Lenin in such an unattractive way?"

Sinyavsky: "I said that you cannot make a cult of Lenin. To me Lenin is a human being; there is nothing wrong about that."

Judge: "What did you mean in this passage about the deification of Stalin?"

Sinyavsky: "I am being ironical about making a cult of him. If Stalin had lived a little longer, it might well have come to that."

And on and on and on, with Mr. Sinyavsky being persecuted and prosecuted for the expression of his views.

To cite the Sinyavsky example is simply and sadly to say that "1984" continues to have more than allegorical relevance in totalitarian states such as the Soviet Union. But the question, Mr. Chairman, I think is whether it has genuine relevance here at home.

And I believe it does. For if our Constitution affords us enormous protection in the areas of freely expressing our opinions and freely telling the truth—even when the Government prefers that we not do so—there are some areas that we cannot look to the Constitution for much in the way of refuge or comfort. They relate to the availability of information itself, the basis of the formation by the public of its views and its expression of them.

In this area we must not look to our almost 200-year-old Constitution but to our living representatives in the Congress and in the executive branch. Of them and of you, I believe the public has much to ask. For if the public does not have information, it cannot play a meaningful role in the formulation of policy. When informa-

tion is suppressed by the Government, the legally guaranteed freedoms to think and to speak become meaningless. Carried to its ultimate end, it would be "1984" without cruelty, without terror, but nonetheless without freedom.

Let me offer some examples. The administration's efforts to censor the speech of former Government officials who have had access to certain kinds of classified information strikes at the heart of the notion that an informed public is an essential ingredient of a free people.

According to the terms of the contract which is to be signed by in excess of 100,000 Government employees and officials, all writings of theirs of any sort that concern explicitly or implicitly intelligence activities, sources or methods must first be cleared by the Government itself for the rest of the lives of those employees.

Such information need not even be classified to be subjected to governmental censorship. Thus, if a former high-level Government employee who would sign such an agreement wanted today to criticize the failure of intelligence in Lebanon or in Grenada, he would first have to clear his statements—even if it contained no classified information at all—with the very people he wanted to criticize.

Orwell would have understood. In response to this risk, we are urged by the proponents of the new censorship agreement to trust the Government to enforce it fairly, to trust the Government not to use it for political purposes, to trust the Government not to censor too much.

Orwell knew better. He teaches us—to put the point mildly—a government can hardly be trusted in judging criticism of itself. Orwell also teaches us that the effect of censorship is a powerless, uninformed, and utterly cynical public. "Who cares," asks Julia, the heroine of "1984," whether the Government was now telling the truth about past events. "It's always one bloody war after another, and one knows the news is all lies anyway."

I referred earlier to the freedom afforded by our Constitution to form and express opinions. But in recent years, and to a lesser extent, still farther back years, that freedom has been frustrated by the use of our Government of the McCarran-Walter Act to deny visas to speakers whose views were sought by American audiences. How can the administration's denial of a visa to Mrs. Hortense Allende, the widow of the former Chilean prime minister, be justified when some of our fellow citizens wish to hear her? Or, more recently, the denial of visas to Sandinista leaders that Members of Congress, among others, wished to hear?

Orwell surely would have understood a mindset which effectively intrudes upon the ability of our citizens, not to say our elected representatives, to decide for themselves what to think after hearing those with whom we may differ.

I could cite numerous other examples which trouble me about the ability of the public to receive information. The exclusion of the press from Grenada at a time when it was especially urgent that the public have nongovernmental information about the invasion; the efforts to limit the flow of information to the public under the Freedom of Information Act; the inhibition of the flow of films into and even out of our country based on their content; revisions in the classification system to ensure that more and not less infor-

mation will be classified; threats to universities with respect to their right to publish and discuss unclassified information.

What I would like to leave you with, Mr. Chairman, is not a catalog of my complaints, but a suggestion as to the way to view expressions of the executive branch that national security requires the denial of information to the public. Only if you view those statements with intense skepticism, with a presumption that a denial of information to the public is, in the most real sense, un-American, will you avoid a serious, continuing deprivation of relevant information by the public.

For the problem is that just about everything worth knowing can be viewed in one way or another as possibly impacting adversely on national security—by discouraging our citizens, by depressing our allies, by running counter to someone's notion of the national interest. Of course, there are some real secrets, but hardly as many as the executive branch would have us believe.

A colleague of mine at the Columbia School of Law, Prof. Vincent Blasi, in a recent speech he gave observed that he thought that the courts in adjudicating first amendment disputes ought to adopt what he called a pathological perspective. The "overriding objective at all times," he argued, "should be to equip the first amendment to do maximum service in those historical periods when intolerance is most prevalent and when governments are most able and most likely to stifle dissent systematically."

I would urge the same perspective on you as you view efforts to deny the public information. You should adopt a view which focuses on the loss to the public of information in the worst of times. You should assume a government at its worst, its most repressive, its least tolerant. George Orwell created for us the model of that government, and as we move toward 1984, I urge upon you that the best way to avoid "1984" is by assuring a public informed enough that it can do so.

Thank you, Mr. Chairman.

[The complete statement follows:]

PREPARED STATEMENT OF FLOYD ABRAMS

Chairman Kastenmeier and members of the subcommittee, I am honored by your invitation to testify today. Apart from my pleasure at being here, I do admire your choice of topic. Indeed, you have chosen as your topic a central one for the future of our country. As we meet virtually on the eve of 1984, the Orwellian nightmare, lucid and terrifying as it is, offers us a basis for learning and for comparison.

Permit me, at the outset, to recall for you Orwell's grim vision of 1984. It is of a nation, Oceania (of which we and the United Kingdom are a part) which is perpetually at war with one or another of the other two superpowers in the world—Eastasia and Eurasia. It is of a society premised on terror, totally dominated by its totalitarian rulers, in which any who differ are tortured, brainwashed and ultimately either vaporized or left, as was the hero Winston Smith, utterly drained of humanity and filled with only those thoughts that the state chose that he have. "If you want a picture of the future," Smith is told by his torturer, "imagine a boot stamping on a human face—forever."

1984 is also a vision of a state with the clearest possible views about the dangers of truth. It is one in which the state had not only redefined falsehood as truth, but in which the definition of truth continually changed. A society in which the hero finds an old newspaper clipping conclusively proving that confessions of three supposed traitors were fraudulent—that they were, in fact, not at the place at which they had confessed to being during their supposedly treasonous act. And in which he then thinks the following to himself:

"There was only one possible conclusion: the confessions were lies."

"Of course, this was not in itself a discovery. Even at that time Winston had not imagined that the people who were wiped out in the purges had actually committed the crimes that they were accused of. But this was concrete evidence; it was a fragment of the abolished past, like a fossil bone which turns up in the wrong stratum and destroys a geological theory. It was enough to blow the Party to atoms, if in some way it could have been published to the world and its significance made known."

Of course, it is never published to the world and the hero himself is later bludgeoned, tortured, and brainwashed into believing that he had never seen the clipping, that it had, indeed, never existed.

It is, of course, not our society. It is worth saying that today. It will not be our society in 1984. Or, we may hope, thereafter.

It is worth pausing for a moment on why that is so. In good part it is because we live under a system of law with a Bill of Rights which protects against just the elements of 1984 we find most offensive—against, in short, a state that directs us, controls us and ultimately rules us. We are—need I say—not tortured because we hold different views than our Government. In fact, so far does our constitutional protection go that truthful statements are almost totally insulated from governmental sanctions of any sort. So far does our protection go that we are free to express any opinion without fear of governmentally imposed sanctions: there is no such thing in this country, Justice Lewis Powell has observed for the Supreme Court, "as a false opinion."

Our law, then, goes far towards protecting us against the 1984 vision becoming a reality. The absence of such legal protection is evident abroad. Consider the public interrogation of the Soviet dissident Sinyavsky, one which—fittingly—could well have been annexed to an updated version of 1984.

Prosecutor: "Please don't lecture us on literature. I ask you a simply concrete question: Why did you portray Ilyich [Lenin] in such an unattractive way?"

Sinyavsky: "I said that you cannot make a cult of Lenin. To me Lenin is a human being; there is nothing wrong about saying that."

Judge: "What did you mean in this passage about the deification of Stalin?" (Reads excerpts.)

Sinyavsky: "I am being ironical about making a cult of him. If Stalin had lived a little longer, it might well have come to this."

Prosecutor: "Do these three words reflect your political views and convictions?"

Sinyavsky: "I am not a political writer. No writer expresses his political views through his writings. An artistic work does not express political views. You wouldn't ask Pushkin or Gogol about their politics. (Indignation in the courtroom.) My works reflect my feelings about the world, not politics."

Prosecutor: "I had a different impression * * *."

And:

Sinyavsky: " * * * I should point out that sometimes he moves away from Lenya and at other times he comes back to him * * *."

Prosecutor: "You are trying to move away from the point!"

Sinyavsky: "I'm not making fun of Communism, but of Proferansov."

And this:

Prosecutor: "Let's go back to your essay on Socialist Realism. Let's take your political views: What did you have in mind when you wrote: 'To do away with prisons, we built new prisons * * *. We defiled not only our bodies, but our souls'? What has this got to do with socialist realism?"

To cite the Sinyavsky example is simply and sadly to say that 1984 continues to have more than allegorical relevance in totalitarian states such as the Soviet Union. Does it have genuine relevance here at home?

I believe it does. For if our Constitution affords us enormous protection in the areas of freely expressing our opinions and freely telling the truth—even when the Government prefers that we not—there are some areas in which we cannot look to the Constitution for much in the way of refuge or comfort. They relate to the availability of information itself, the basis of the formation by the public of its views and its expression of them. In this area, we must look not to our almost 200-year old Constitution but to our living representatives in the Congress and in the executive branch. Of them, of you, I believe the public has much to ask.

For if the public does not have information, it cannot play a meaningful role in the formulation of policy. When information is suppressed by the government, the legally guaranteed freedoms to think and to speak become meaningless. Carried to its ultimate end, it would be 1984 without cruelty, without terror, but nonetheless without freedom.

Let me offer some examples. The administration's efforts to censor the speech of former Government officials who have had access to certain types of classified information strikes at the heart of the notion that an informed public is an essential ingredient of a free people. According to the terms of the contract (which is to be signed by in excess of 100,000 Government officials and employees) all writing of theirs of any sort that concern—explicitly or implicitly—"intelligence activities, sources or methods" must first be cleared by the government itself for the rest of the lives of those employees. Such information need not even be classified to be subjected to Government censorship. Thus, if a former high-level Government official who had signed such an agreement wanted today to criticize a failure of intelligence in Lebanon leading to the death of our Marines or of one in Grenada, he would first have to clear his statement—even if it contained no classified information at all—with the people he wanted to criticize. How George Orwell would have understood.

In response to this risk, we are urged by the proponents of the new censorship agreement to trust the Government to enforce it fairly, to trust the Government not to use it for political purposes, to trust the Government not to censor too much. Orwell knew better. He teaches us—to put the point mildly—that Government can hardly be trusted in judging criticism of itself. Orwell also teaches us that the effect of censorship is a powerless, uninformed and utterly cynical public. "Who cares," asks Julia, the heroine of 1984, whether the government was now telling the truth about past events. "It's always one bloody war after another, and one knows the news is all lies anyway."

I referred earlier to the freedom afforded by our Constitution to form and express our opinions. But in recent years (and, to a lesser extent, previous years) that freedom has been frustrated by the use by our Government of the McCarran-Walter Act to deny visas to speakers whose views were sought by American audiences. How can the administration's denial of a visa to Mrs. Hortense Allende, widow of the former Chilean Prime Minister, be justified when some of our fellow citizens wish to hear her? Or, more recently, the denial of visas to Sandinista leaders that Members of Congress, among others, wished to hear? Orwell surely would have understood a mindset which effectively intrudes upon the ability of our citizens, not to say our elected representatives, to decide for themselves what to think after hearing those with whom we may differ.

I could cite numerous other examples which trouble me about the ability of the public to receive information: the exclusion of the press from Grenada at a time when it was especially urgent that the public have nongovernmental information about the invasion; the efforts to limit the flow of information to the public under the Freedom of Information Act; the inhibition of the flow of films into and even out of the country based on their content; revisions in the classification system to assure that more and not less information will be classified; threats to universities with respect to their right to publish and discuss unclassified information. I have already set forth my views on most of these matters in a recent magazine article (New York Times Magazine, September 25, 1983) and will not burden you with a repetition of them now.

What I would like to leave you with is not a catalogue of complaints, but a suggestion as to the way to view expressions of the executive branch that national security requires a denial of information to the public. Only if you view those statements with intense scepticism, with a presumption that a denial of information to the public is, in the most real sense, un-American, will you avoid a serious, continuing deprivation of relevant information by the public. For the problem is that just about everything worth knowing can be viewed, in one way or another, as possibly impacting upon national security—by discouraging our citizens, by depressing our allies, by running counter to someone's notion of the national interest. Of course, there are some real secrets, but hardly as many as the executive branch would have us believe.

A colleague of mine at the Columbia University School of Law, Professor Vincent Blasi, has given an extraordinary speech that I would like to mention in conclusion. First delivered at Columbia earlier this year (and now being prepared in article form) it was entitled: The First Amendment in the Worst of Times. Simply put, Professor Blasi's thesis was that courts, in adjudicating first amendment disputes, ought to adopt what he called a pathological perspective. The "overriding objective at all times," he argued, "should be to equip the First Amendment to do maximum service in those historical periods when intolerance is most prevalent and when governments are most able and most likely to stifle dissent systematically."

I would urge the same perspective on you as you view efforts to deny the public information. You should adopt a view which focuses on the loss to the public of information in the worst of times. You should assume a government at its worst, its

most repressive, its least tolerant. George Orwell created for us the model of that government. As we move towards 1984, I urge on you that the best way to avoid 1984 is by assuring a public informed enough to do so.

Mr. KASTENMEIER. Thank you, Mr. Abrams.

Before we ask you to take questions, I would ask our next panel to join you at the witness table, and perhaps you could remain there and entertain questions when they do.

We cannot help but take note that we begin these hearings in the shadow of the war in Grenada, where restriction of press coverage is seen as illustrative of the problems posed by restrictions of flow of information. This is not a partisan issue. Although it did occur under this administration, it could certainly occur under future administrations. While the events in Grenada are too timely to ignore, I hope they can be viewed in a broader context than our hearings will present.

I would like to present a most distinguished group of individuals: Mr. Edward M. Joyce, president of CBS news, who has had an outstanding career as a news executive and award-winning reporter. He has been with CBS since 1954. Next, John Chancellor, senior commentator for NBC Nightly News and one of the most respected journalists in broadcasting. His 30-year career with NBC has been marked by well-deserved recognition for his outstanding contributions to television news.

Finally, David Brinkley, senior correspondent with ABC news. His name is virtually synonymous with the best of broadcast reporting. During his 40-year career, he has won every major broadcasting award, including 10 Emmys.

Gentlemen, we are most pleased to have the benefit of your testimony this morning. Mr. Joyce, you may proceed.

TESTIMONY OF EDWARD JOYCE, PRESIDENT, CBS NEWS, JOHN CHANCELLOR, SENIOR COMMENTATOR, NBC NEWS, DAVID BRINKLEY, SENIOR CORRESPONDENT, ABC NEWS

Mr. JOYCE. Thank you. I welcome the opportunity to present the views of CBS News on the restrictions imposed on press coverage of Grenada. On October 25, the United States and six Caribbean nations invaded the island of Grenada. On that day the United States introduced a new relationship with the press, a relationship virtually unknown in U.S. history. The press restrictions imposed by our Government on Grenada news coverage prevented the press from gathering and reporting to the public. By denying access as the Government did in Grenada, it also denied to the public the ability to receive information gathered by an independent press. Instead, the American public received only the information the Government wanted it to receive. This is not what a free society is all about.

From the outset, the Government declared that it was not safe for the press to be in a war zone. Thus, at a time when CBS news had more than 2 dozen of its people in war-torn Lebanon, we were told that we could not go to Grenada because the military could not guarantee our safety.

But whatever the rationale, the public, which received firsthand information from the press in Vietnam, in Korea and in World War II, was denied firsthand reporting from Grenada. I submit

that is intolerable. I want to emphasize that the American press is a responsible press. We are not seeking to report military secrets. We are not seeking to jeopardize lives. But those interests could have been protected without resorting to the unprecedented censorship that the President imposed in Grenada.

Last Sunday the military commander of the American task force in Grenada said the decision to keep out the press was his, that it would do no good to protest at higher levels. Indeed, the Secretary of Defense last week said that he would not overrule the military on this issue. Last week a number of us watched his satellite feed in which an Australian journalist told his countrymen, we have just seen the end of 200 years of press freedom in the United States. I hope that the Australian journalist was overreacting. But I am seriously concerned that we may indeed be witnessing the dawn of a new era of censorship, of manipulation of the press, of considering the media the handmaiden of Government to spoon feed the public with Government-approved information.

If the Government is permitted to abrogate the first amendment at will to the detriment of not simply the press but the public as well, I am concerned that such action will be taken again and again and again whenever a government wishes to keep the public in the dark.

I find it ironic that this hearing is taking place 1 month to the day after representatives of some 60 print and broadcast organizations from 25 countries meeting in Talloires, France, condemn attempts to regulate news content. That meeting was arranged, in part, by American press groups, notably the World Press Freedom Committee, and included Third World countries. They were attacking efforts to regulate news content, then largely led by the Soviet Union.

The press has covered virtually every war fought by this country. In its coverage, the press has served as a ratifying factor in reporting to the public what has occurred. Indeed, from World War II to now, more than 125 correspondents have been killed while covering wars in which the United States has been involved. We do not cover wars from hotel rooms far behind the lines of battle. We do not wish to cover wars on the basis of handouts from the Pentagon.

One CBS news correspondent was told by two colonels at the Pentagon that, "We learned a lesson from the British in the Falklands." Well, that lesson was censorship. CBS news protested that action in a letter to the Secretary of Defense on October 25. There has been no reply.

On the third day of the invasion, the Pentagon began to release its own film, which clearly represented what the Government wanted the public to see and believe. It may have been an accurate portrayal. Without the presence in Grenada of a free and independent press, America will never really know.

When the press was finally admitted to Grenada, for several days it was compelled to operate in the most limited and restricted fashion. We saw what our Government wanted us to see, when our Government wanted to see it, for as long as our Government deemed appropriate. It was not until the sixth day of the invasion that the press was allowed to cover Grenada in a more meaningful fashion.

We at CBS news are concerned, frustrated, and saddened by the press restrictions of the past week. We are concerned by the repressive actions of the Government toward the press. We are frustrated because we were not able to do the reporting job the public expects of us and we expect of ourselves. And we are saddened to bear witness to this new, unchecked censorship leading to an off-the-record war.

Thank you, Mr. Chairman.
[Complete statement follows:]

PREPARED STATEMENT OF EDWARD M. JOYCE, PRESIDENT, CBS NEWS

I welcome the opportunity to present the views of CBS News on the restrictions imposed on press coverage of Grenada.

On October 25, the United States and six Caribbean nations invaded the island of Grenada. On that day, the U.S. introduced a new relationship with the press, a relationship virtually unknown in U.S. history.

The press restrictions imposed by our Government on Grenada coverage prevented the press from gathering and reporting the news to the public. By denying access, as the Government did in Grenada, it also denied to the public the ability to receive information gathered by an independent press. Instead, the American public received only the information the Government wanted it to receive. This is not what a free society is all about.

From the outset, the Government declared that it was not safe for the press to be in a war zone. Thus, at a time when CBS News had more than two dozen of its people in war-torn Lebanon, we were told that we could not go to Grenada because the military could not guarantee our safety. But whatever the rationale, the public—which received first-hand information from the press in Vietnam, in Korea, and in World War II—was denied first-hand reporting from Grenada. I submit that is intolerable.

I want to emphasize that the American press is a responsible press. We are not seeking to report military secrets. We are not seeking to jeopardize lives. But those interests could have been protested without resorting to the unprecedented censorship that the Government imposed in Grenada.

Last Sunday, the military commander of the American task force in Grenada said the decision to keep out the press was his, that it would do no good to protest at higher levels. Indeed, the Secretary of Defense last week said that he would not overrule the military on this issue.

Last week a number of us watched a satellite feed in which an Australian journalist told his countrymen we have just seen the end of 200 years of press freedom in the United States.

I hope that the Australian journalist was overreacting, but I am seriously concerned that we may indeed be witnessing the dawn of a new era of censorship, of manipulation of the press, of considering the media the handmaiden of government to spoon feed the public with Government-approved information. If the Government is permitted to abrogate the first amendment at will, to the detriment of not simply the press but the public as well, I am concerned that such action will be taken again and again, whenever a Government wishes to keep the public in the dark.

I find it ironic that this hearing is taking place 1 month to the day after representatives of some 60 print and broadcast organizations from 25 countries, meeting in Talloires, France, condemned attempts to regulate news content. That meeting was arranged, in part, by American press groups, notably the World Press Freedom Committee, and included third world countries. They were attacking efforts to regulate news content, then largely led by the Soviet Union.

The press has covered literally every war fought by this country. In its coverage, the press has served as a ratifying factor in reporting to the public what has occurred. Indeed, from World War II to now, 125 correspondents have been killed while covering wars in which the U.S. has been involved. We do not cover wars from hotel rooms far behind the lines of battle; we do not wish to cover wars on the basis of hand-outs from the Pentagon.

One CBS News correspondent was told by two colonels at the Pentagon that we learned a lesson from the British in the Falklands. That lesson was censorship. CBS News protested that action in a letter to the Secretary of Defense on October 25. There has been no reply.

On the third day of the invasion, the Pentagon began to release its own film which clearly represented what the Government wanted the public to see and believe. It may have been an accurate portrayal. Without the presence in Grenada of a free and independent press, America will never really know.

When the press was finally admitted to Grenada, for several days it was compelled to operate in the most limited and restricted fashion. We saw what our Government wanted us to see, when our Government wanted us to see it, for as long as our Government deemed appropriate.

It was not until the sixth day of the invasion that the press was allowed to cover Grenada in a more meaningful fashion.

We at CBS News are concerned, frustrated, and saddened by the press restrictions of the past week.

We are concerned by the repressive actions of the Government toward the press. We are frustrated because we were not able to do the reporting job the public expects of us and we expect of ourselves.

We are saddened to bear witness to this new, unchecked censorship, leading to an off-the-record war.

Mr. KASTENMEIER. Thank you, Mr. Joyce.

And now John Chancellor.

Mr. CHANCELLOR. Mr. Chairman, I will not take much of your time this morning. I am glad the subcommittee asked me to appear because I think the problem that is being considered today affects one of the basic elements of a free society. It is not only the privilege of the American press to be present at moments of historic importance, it is the responsibility of the press to be there.

The men who died in the invasion of Grenada were representing values in American life. One of those values is the right of the citizenry to know what their Government is doing and to learn that from a free and independent press. That principle of the press as an observer and a critic of the Government was established at the beginning of the United States, and it is the responsibility of all citizens to uphold it.

For the subcommittee's convenience, I have attached two commentaries I wrote on these topics for the NBC Nightly News, although I appear here today as a private citizen and not a representative of the National Broadcasting Co. Thank you.

[The complete statement follows:]

PREPARED STATEMENT OF JOHN CHANCELLOR, SENIOR COMMENTATOR, NBC NEWS

I am glad the subcommittee asked me to appear at this hearing, because I think the problem that is being considered today affects one of the basic elements of a free society.

It is not only the privilege of the American press to be present at moments of historic importance, it is the responsibility of the press to be there. The men who died in the invasion of Grenada were representing values in American life; one of those values is the right of the citizenry to know what their Government is doing, and to learn that from a free and independent press. That principle, of the press as observer and as critic of the Government, was established at the beginning of the United States. It is the responsibility of all citizens to uphold it.

For the subcommittee's convenience, I have attached two commentaries I wrote for the NBC Nightly News which express my views, although I appear here today as a private citizen and not a representative of the National Broadcasting Co.

Well, there's one thing you can say about the invasion of Grenada; it isn't a living room war.

There are American troops in combat, fighting with Cubans, putting Russians into custody—and not a single member of the American press allowed to observe.

The American Government is doing whatever it wants to in Grenada without any representative of the American public watching what it's doing. No stories in your newspapers or magazines; no pictures in your living room.

When the British went into the Falklands they allowed a few correspondents and cameramen to go along, a small tip of the hat to a free press. But in Grenada, the

Reagan administration has produced a bureaucrat's dream: do anything, no one is watching.

It would have been easy for the Pentagon to take some press people along, with no security risk.

But that's not the way the Reagan administration operates.

It lied to its own White House Press Office about Grenada.

It don't consult the Congress, only informed it, and it ducked the serious parts of the War Powers Act.

This passion for secrecy is no surprise. Earlier this year, again without consulting the Congress, the President put out the most sweeping and dictatorial censorship directive in the history of the American Government. From now on, anyone who reads certain classified documents is subjected to censorship for life. It is so bad that the Senate has come out against it and the House is expected to.

The Secretary of Defense explains American casualties in Grenada by saying, The price of freedom is high.

What freedom? The freedom of the American people to know what their Government is doing?

This administration clearly doesn't believe in that.

It is being said this week that the American government did two good things when it invaded Grenada; it beat the commies and kept out the press. The exclusion of the press from the early days of the fighting is being cheered by some people.

We are told that the decision to keep the press out was a purely military decision. That is hard to believe. There is a long and honorable tradition of cooperation between the American military and the American press. Never before has the press been excluded from a military operation of this size; the decision to keep the reporters away got into the area of politics. If there is one thing sure about life in America it is that the military doesn't make political decisions on its own.

We are told that the press was kept away from Grenada for its own safety. That, too is hard to believe. Danger is part of the job. The overseas press club says that since 1940, 123 members of the press have died in combat covering American forces. Their safety, or the lack of it, was up to their own news organizations. Journalists in combat zones sign waivers absolving governments from responsibility. The Israelis had me sign one in Lebanon last year. It's the way things work and it's the only way that free and accurate coverage of combat can be guaranteed.

When there's a war on, journalism can be a risky business for journalists.

But no journalism at all is risky for the country. The press, good or bad, and it's both, is a necessary part of the process of democracy.

Every once in a while the press gets it in the neck, which is probably healthy. But the people who are happy that the press was kept off Grenada while the fighting went on ought to ask themselves: do you know where your Government is, and what it's up to? Without the press, you can only put your faith in the official version.

Mr. KASTENMEIER. Thank you, Mr. Chancellor.

And now, Mr. David Brinkley.

Mr. BRINKLEY. Mr. Chairman and members of the committee, speaking for ABC News, I would like to thank you for allowing us to appear.

We have been given two reasons for the Defense Department's refusal to allow reporters in Grenada: First, the security of the operation itself; second, safety of the reporters themselves.

As to the first, security could easily have been maintained by the armed services by controlling, as they do control, all means of communication between Grenada and the United States. Beyond that, reporters could have been taken ashore an hour or so after the operation began and when it was no longer a secret.

As for the second point, physical safety of the reporters, every one in our business has always understood there is risk and danger in covering military operations and in the past everyone of us has been willing to sign a statement relieving the military of any responsibility for us. Everyone understood that in Vietnam, where I believe more than 100 journalists were killed and many more injured and no one to my knowledge has ever attempted to blame the

military. So security could easily have been controlled, as it has been in the past.

As for the physical safety of our reporters, that is a question the military has raised. But we never have. Probably it is in the nature of military commanders, their profession being what it is, to want theater operations to be cleared of all but military people. Civilians, including the press, I suspect are seen as an impediment, excess baggage, generally in the way, and therefore not welcome.

Well, we place great responsibility upon our military leaders and demand of them a very high level of performance in difficult circumstances. And in that light, their attitude may, to some extent, be understandable. But in my view, it is still bad policy, since any military operation is carried on in behalf of the American people. And if military leaders are to have, as they must have, the support of the American people then they must know what it is they are asked to support.

There is nowhere they can learn that but from us. And they cannot learn it from us if we are not allowed to go there.

To conclude, I would like to quote Gen. Edward C. Meyer, who retired this year from the Joint Chiefs of Staff, who said, "Soldiers should not go off to war without having the Nation behind them." Thank you.

[The complete statement follows:]

PREPARED STATEMENT OF DAVID BRINKLEY, SENIOR CORRESPONDENT, ABC NEWS

Mr. Chairman and members of the subcommittee: I have been reporting news from Washington for many years. I first came to Washington in 1943 and I have covered national political affairs and public policy ever since for both print and broadcast news organizations. Through the years there have been many disputes between Government and the press regarding the right of the press to look into every corner of the Government in its search for news. The Government, no matter who is in the White House, has resisted this relentless poking about and has tried to limit journalists wherever it could. So the events of last week when the White House and Pentagon severely restricted the flow of information from Grenada is just one more unfortunate example of Government's attempts to restrict the press. My own company, ABC News, was among the first to complain about the problems of covering the operation in Grenada. **Roone Arledge** wrote as follows to Secretary of Defense Weinberger on October 25, last Tuesday, the day the Rangers and Marines landed:

Dear Secretary Weinberger: I am seeking your assistance and approval in allowing NBC News correspondents, camerapersons, and producers to cover the military operation of well over 1,500 American combat forces on the island of Grenada.

The problems we are encountering are largely logistical. We would, of course, be willing to pay our own way, provide our own transportation by sea or air, and accept such risks we might now encounter on Grenada. I can assure you that only our most experienced broadcast journalists and technicians would be assigned to this coverage. The problem at this point is permission from the Department of Defense.

I might argue—but I won't—that the practice of journalists accompanying American military units into action is as old as our Nation and as old as the U.S. Marines—and that the Constitutional framers gave special consideration to the function of press in free society.

Suffice it to say that the U.S. troops on Grenada deserve as much coverage as the debate in Washington over their presence there.

Awaiting your reply.

Sincerely, **Roone Arledge**.

There have been two basic themes in the Pentagon's resistance: The first is security of the operation; the second is the safety of the journalists who are covering it. Our rationale for opposing them on the second point is outlined in the letter and I won't add to it here beyond saying that in Vietnam we took our chances in the field with the troops and 53 newsmen were killed or are missing in the course of covering that war. An unknown number were wounded. The best estimate on that score is

150 according to writer Peter Braestrup who has studied press and military operations in Vietnam very closely.

The military could and should have taken journalists ashore on Grenada shortly after the initial assault or even the next day. But so far as we can determine—and perhaps the subcommittee would like to get testimony from the Defense Department on this point—there was never any plan for dealing with journalists.

On the matter of the security of the operation: Newsmen could have been taken in with the first wave with the understanding they would not file until after the operation had commenced. This was frequently done in Vietnam and so far as I know there was never a compromise of a U.S. military operation traced to a journalist. ABC News and other news organizations have been ready, willing, and able to charter planes and boats into the island so that arguments that the military could not support newsmen logistically, are simply specious.

Going back to the parallels in Vietnam, there is no doubt that the press and the military commander in Vietnam, General William Westmoreland, have differed on many points regarding the war, but there is no record of Westmoreland ever accusing the press of compromising the security of the men he commanded.

That's a remarkable record when you consider the length of the war in Vietnam, the numbers of newsmen who covered it and the fact that they were allowed to roam freely about the country and write what they saw without censorship and with only the loosest of guidelines regarding what subjects were proscribed, e.g. future military operations, casualties, troop strengths and movements.

Finally it seems to me that in a Democratic society it is essential that the people have access to information regarding the intentions and the actions of their government. This is particularly true in the case of military operations when men and women are asked to support or at least to understand a policy that may lead to the loss of their own lives or the lives of their loved ones. Last June when he retired from the Army after a distinguished career as Chief of Staff, General Edward C. Meyer said, "Soldiers should not go off to war without having the Nation behind them." To which I would simply add, Amen General.

Mr. KASTENMEIER. Thank you, Mr. Brinkley.

Do the three distinguished representatives from the television networks believe that the print media joins you in this concern that you so eloquently reflect today, Mr. Joyce?

Mr. JOYCE. I think it is clear from editorials in newspapers across the country that this is a concern that is mediawide. The "press" we have used today is an all-inclusive phrase to include both print and broadcast.

Mr. CHANCELLOR. Mr. Chairman, the American Newspaper Publishers Association has condemned this. The American Society of Newspaper Editors has condemned this action. I think there is no question that the media, as they are called in the United States, are wholly together on this question.

Mr. KASTENMEIER. I will ask one more question and then I will yield to anyone who remains. To what extent is this action unprecedented, or is there precedent for it in American history? And to what extent does the fact that this was a unique operation, a brief operation involving an invasion of a small island in the Caribbean, make the situation so unique as to potentially justify the exclusion, at least in the early days, of journalists?

Mr. JOYCE. If I could begin a response and then share the table with my colleagues here. I asked that a call be placed to Bert Quint, a CBS news correspondent now based in Warsaw, Poland, for us. Bert covered the 1965 invasion of the Dominican Republic. We asked Bert what the circumstances were. He said that he traveled from Puerto Rico by landing craft to the helicopter carrier *Boxer* and was allowed ashore 2 hours after the Marines. The Navy flew his film each day to Puerto Rico.

I also talked to a CBS news producer, Sam Roberts, who says he was flown into the Dominican Republic from Puerto Rico within 8 hours after the invasion began. That is one example.

If you go back to the example of the Second World War, in April 1944, the Supreme Headquarters Allied Expeditionary Force set forth a governing principle for field press censorship, that the minimum amount of information will be withheld from a public consistent with security.

If we take the example of Vietnam, where censorship was done on a voluntary basis—and my source for this is Barry Zorthian, who was the chief press officer for the U.S. Government during the period of the Vietnam war—in Vietnam accreditation for journalists was lifted for security breach only six times in over 4½ years in dealing with approximately 2,000 news media representatives.

That there is often a tug of war between the military and the press is an inescapable fact. During the Civil War, General Halleck excluded reporters from one zone of conflict, but that was one zone of a larger conflict, and correspondents did cover that war.

In 1813 Thomas Jefferson wrote that the first misfortune of the Revolutionary War induced emotion to suppress the account of it. "It was," he says, "rejected with indignation," which tells you something, I think something about the history of censorship and something about the concept of the Founding Fathers of this Nation in terms of the press and the military.

Mr. KASTENMEIER. Thank you.

I yield to the gentleman from California, Mr. Moorhead.

Mr. MOORHEAD. Thank you, Mr. Chairman.

I certainly want to welcome every one of you here this morning. We appreciate your coming and giving this testimony. But I think in view of the fact that each one of you believes that there should not be censorship, both sides should be presented on each issue. I think that there is another side to the issue, and I think it should be pressed.

Usually, we have opening statements on both sides as well in this kind of a hearing. I must admit that I find it more than a bit alarming that we are meeting this morning to discuss, in part, freedom of the press and sharing of information, and yet it was not until yesterday morning that we in the minority found out that there was going to be such a hearing stressing the Reagan administration's handling of press coverage in Grenada. And we read about it in the Washington Post. So if we had not been reading the newspaper, we might not have known about it even then.

Having said that, Mr. Chairman, I think the central issue before us today is whether or not secrecy was needed to assure the safety of American fighting men and protect the lives of the very people we were being sent to rescue. I believe that it was, or at least that a good case can be made for it.

This was a rescue mission utilizing commando tactics against an enemy that wore civilian clothes and drove civilian vehicles. There was no clear battle line. In other rescue missions in recent memory, such as the Israeli raid on Entebbe and the attempted Carter rescue mission in Iran, the need for secrecy was recognized as paramount. And the press was excluded. Yet the American

public was provided a full accounting of the events after the need for secrecy had passed.

By denying access to the press, the American commander on Grenada ensured the safety of his men and the people he was sent to rescue. We are all aware that the first amendment to the Constitution recognizes the right of free speech and the right of the press to print anything it wants. However, there seems to be some who fail to recognize that it does not guarantee access to information which would jeopardize the safety of Americans.

In the last few days we have heard correspondents broadly state that the press has covered all the Nation's wars, including World War II, the Korean war, and Vietnam. This assertion leaves out several important facts. In World War II you had a system of war correspondents who actually wore uniforms, were given the courtesy rank of an officer, and were subjected to censorship.

When the Korean war started, commanders did not impose censorship, but when reporters were denied access to the peninsula, newsmen asked that censorship be imposed.

Even Vietnam, with no censorship, was not entirely open to the press. Reporters were not along on many of the more important and daring missions. As yet another example, reporters could only cover the air war in Thailand by special permission; they were not allowed free access to the Thai bases.

We will hear testimony today from Ed Joyce that on the third day of the invasion the Pentagon began to release its own film which clearly represented what the Government wanted the public to see and hear. On this point I think it is important to note that the Pentagon was handing over its tapes unedited, which were shot by young soldiers with no political bias.

In only two instances did the Pentagon edit out small segments of the material. At the time the tapes were released, the Pentagon explained to the networks what the two pieces were. One was two soldiers exchanging a password and countersign, which no responsible media would want to divulge; the second segment contained pictures of classified communications equipment which were filmed at the Pope Air Force Base in North Carolina before the operation even began. Clearly, there was no attempt to influence the reporting of events occurring in Grenada by the Pentagon.

One final point concerns the fact that informal polls conducted by several media outlets around the country shows public support for the military decision on press access to Grenada by a margin of almost 2-to-1. For instance, yesterday in our Nation's capital, channel 9 conducted a poll asking the question of whether or not the military was correct in restricting press access. Viewers responded 68 percent in favor of the military decision and 31 percent against.

I think the media needs to listen to the public on some of these issues. But I do want to congratulate you on constantly fighting to get the news and to get the facts. And I do not blame you one bit for asserting the position that you do, because I do think that it is important that the public have all the information on all kinds of issues that they possibly can get and that both sides, even the minority, be allowed to be heard.

Thank you, Mr. Chairman.

Mr. BRINKLEY. Mr. Moorhead, can I respond to that? You say the polls showed the public siding with the military by 2-to-1. I am a little surprised. I thought it would have been 10-to-1. We are not the leaders in the popularity contests in the U.S., and we are well aware of it—

Mr. MOORHEAD. Neither are we.

Mr. BRINKLEY [continuing]. We are well aware of it.

Mr. KASTENMEIER. We do have a vote on the floor. We have about 3 or 4 minutes to make it. You may want to comment on Mr. Moorhead's observations, eloquently presented, reflecting the administration's position, but in view of the fact there is a vote on, we will recess, for about five or 10 minutes.

The committee stands in recess.

[Recess.]

Mr. KASTENMEIER. The committee will reconvene.

The Chair would now like to yield to the gentleman from Oklahoma, Mr. Synar.

Mr. SYNAR. Thank you, Mr. Chairman, very much.

First of all, let me welcome all four of our panelists this morning. I appreciate your comments because, as a Congressman who went through the 48 hours during the invasion, not only were you all deprived of information, but the information which we were able to obtain from DOD and the briefings we had was, at best, very limited.

I have been concerned as a Representative whether or not I can accurately or informatively keep my people back in Oklahoma informed on what is going on, based upon the fact that we have had limited information coming to us as Members of Congress and almost no information coming to the press.

Let me ask you, Mr. Brinkley—and I am not old enough for this, and I am not saying that we are showing age—but am I correct that the press accompanied the bombing of Hiroshima and also accompanied the invasion during D-day and that there were no leaks on either one of those occasions?

Mr. BRINKLEY. The two great secrets of World War II were the date of the invasion of France and the dropping of the atomic bomb.

In the case of the invasion of France, the press was informed well in advance. It went ashore with the troops, was shot at, killed, along with everyone else. There was no leak.

In the case of the dropping of the atomic bomb, the second great secret of World War II, a reporter went along on the airplane that dropped the bomb, because the War Department—it was then—felt someone, when it was all over, had to explain it to the public, and they took a reporter specializing in science topics from the New York Times, took him along, and after it was all over he wrote several long articles in the Times explaining a concept that none of us had ever heard of before. It worked effectively; there were no leaks.

Mr. SYNAR. I appreciate that, and I appreciate, Mr. Chairman, these hearings today because I think they are very important. I share the concern of the chairman and the panelists this morning of the ability of the American public, which will have to support any encounter like this, to be well-informed with accurate information.

I am reminded of Thomas Jefferson's comments as well. He said, to paraphrase him, that if he had a choice between the form of government which we have and the press he would choose the press every time. Maybe in this instance this is an example of where that statement holds true.

Thank you very much, Mr. Chairman.

Mr. KASTENMEIER. I thank the gentleman from Oklahoma.

The gentleman from Kansas, Mr. Glickman.

Mr. GLICKMAN. Thank you, Mr. Chairman.

In addition to the first amendment questions, on which I fully agree with my colleague from Oklahoma, I have some questions regarding the kinds of information that we ultimately did get, which came from the military. I have great concern about the flow and the quality of information that came from the military, and my question is: Can we trust that information?

We didn't hear anything about the bombing of the mental hospital for several days after it had occurred, and once we heard about it, it was denied.

The information on the troop strength was wrong, and I suppose this comes back to the fact that there was not an independent source of information there at the time.

But I would ask the question: Can we trust the information that we are getting?

Mr. CHANCELLOR. Well, I can respond to that. I think you can, in all probability, Congressman, trust the information that the Department of Defense put out, but that was selectively released information, it seems to me.

When I was working for the USIA here in Washington, we used to have meetings in which we would outline themes to be stressed to make the American Government look more powerful, more sympathetic, more intelligent, more understanding, and these themes would be stated in position papers, and anybody who knows the propaganda business knows that that is how it works.

Now, nothing that we said at the USIA was ever untrue, but it was the arrangement of the truthful information that made the point, and I think in this case we saw certain themes that the Government wanted us to see.

We saw pictures that were quite clear and accurate and truthful of a warehouse filled with boxes of arms that had Russian Cyrillic markings on them. We saw troops in civilian clothes—that were described as troops—I presume they were. They didn't look like troops to me, but I can accept that. And as far as the hospital is concerned and the shifting numbers of order of battle figures, I think that happens in any large military operation.

But the themes were there.

Mr. JOYCE. If I could add to that, I think there are a host of questions for which we do not have independently verifiable answers, such as who fired first. The Cubans are saying that they gave word to their troops not to fire first.

How stiff was the Cuban opposition? Over 600 prisoners out of a total fighting force of between 700 and 800 does not give the impression of having fought to the last man.

What happened to the Grenadan Army? There are no reporters who can really answer that for us.

And I would like, if it is appropriate, just to respond to a couple of points that Congressman Moorhead brought up.

Mr. GLICKMAN. Well, I don't have very much time. If possible, let me just ask a couple more questions, and then if there is time the chairman will go back around again.

I would just like to come back on a point that Congressman Synar asked you, Mr. Brinkley, about the censorship of press in previous restrictive and secretive activities.

In any of the modern memory of the folks sitting at the table today, has the media ever been restricted before in the same way that you are restricted in Grenada?

Mr. BRINKLEY. Not to my knowledge.

Mr. JOYCE. Not to my knowledge. I can't recall exclusion from a total area of conflict.

Mr. CHANCELLOR. I think the answer is that the United States sent a task force of 15,000 people to invade a sovereign country. No military operation of that size, in my experience and in my reading of American history, has ever been done without the accompaniment of the American press.

Mr. GLICKMAN. OK, one final question. The Secretary of Defense and others seem to imply that there is some danger in taking the press into their confidence. Is there any such danger?

Mr. BRINKLEY. There is nothing in the record to suggest it, Congressman. As I have said, in military operations in the past, including many a great deal bigger than this, the press has been taken into the military's confidence in advance, and there have been no leaks.

But beyond that, in those cases, as in this case, the armed services controlled communications between the battle scene and the outside, and so if there were a leak it would be very hard for it to go anywhere.

Mr. JOYCE. Congressman, it is important to remember that even if there had been initial secrecy that still does not explain or justify the information blockade that was maintained for days. Even if several hours had gone by with an invasion which had taken place in secrecy, obviously no plans had been made—or I will contradict myself—apparently, plans had been made to bar the press from access to that island.

Mr. GLICKMAN. Thank you, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from Ohio, Mr. DeWine.

Mr. DEWINE. I am still out of breath, Mr. Chairman, from running back from the vote. Thank you very much.

Mr. KASTENMEIER. I hope you made it.

Mr. DEWINE. I did, yes, sir. Thank you.

It seems to me, aren't we really, gentlemen, dealing with a balancing test? Don't we in society balance every day certain interests along with the question of access?

I am not saying we balance freedom of speech or freedom of the press, but when we are talking about access, don't we balance that?

Now, the absurd example, which may not relate at all to this, is a suicidal person who is going to jump off a 10-story building. There may be some attempt to rescue that person by the police. The press would not necessarily be right there on the scene.

I mean, it seems to me it is a balancing test, for example, the situation that other countries have had, such as the Israelis/Entebbe situation or the aborted Iranian rescue of the United States. I would like your comments on this and see if you agree with my basic premise—that what we are really talking about today is how those interests are balanced and at what point the access should be granted.

It seems to me that what you are saying is that access should have been allowed much earlier in this situation than it was. The administration would look at the different days and say on the third day there were so many journalists and on the fourth day there were so many. What you are saying is they should have been in at a much earlier point.

Is that a fair statement? I mean, you are not saying, are you, that there is a total right to access?

In other words, I don't think the American people would accept the premise that if the safety of an American soldier would in any way be jeopardized by the press' presence that their right to know, the people's right to know, would take precedence over getting an American soldier killed.

We may not be dealing with that situation here, but just to take it to its final example.

Could you comment on that?

Mr. BRINKLEY. Well, the American people would not accept that, and neither would we. We have never advocated any such thing.

Again, in the case of the Grenada invasion there probably was reason for secrecy so as to achieve surprise. There was, nevertheless, a leak, which was down in the Caribbean. It didn't come from here, and it was all announced in a Caribbean newspaper the day before.

Secrecy, again, could have been protected by the military keeping control of communications, which it had and still has.

Mr. JOYCE. Congressman, there was no outcry when the raid, which failed, the raid to release hostages from Tehran took place. There was no outcry that a pool camera was not aboard one of the helicopters.

So I think your point has merit.

Mr. ABRAMS. Congressman, can I just add that it seems to me that when you talk about rescue operations such as Entebbe and Iran, that you do have to say that the balance is a different sort than is involved here.

If this had been an in-and-out rescue effort—American troops landed, picked up students, and got out—I think we would have a very different situation. Here was a full-fledged military force remaining on the ground and occupying a country, and I think that that should be borne in mind as you try to strike a balance in terms of when the press was allowed in to start reporting independently to the American public.

Mr. CHANCELLOR. Congressman, I think one important point here is that there are established procedures that go back many years for guaranteeing that the press not report an important story. The difference is that the press is allowed to be there and report it later.

When President Johnson visited Southeast Asia in, I think, 1966, the press, a pool of reporters accompanying him, was called into a hotel room in Manila by the White House Press Office. The door was locked. They were told they were going to Cam Ranh Bay with the President. They all walked out another door, virtually under guard. Nobody complained. They went to Cam Ranh Bay. Security was not broken on that at all.

But the important thing for the American people was that the press was there to observe the President in a combat zone, and the press came back and told the American people about it.

It doesn't have to be done the same day, and it doesn't have to be done the same week.

Mr. DEWINE. OK, that was, I guess, my point, and the response I was trying to get from you was that at what point should that take place. That, really, is what we are talking about here today.

Mr. Chairman, if I could just have one last question for Mr. Joyce, and, Mr. Joyce, this is something that has bothered me for the last several days, and I have the opportunity today to ask you about it and I wish you could respond maybe to set my mind at ease, or not. I don't know.

But I heard over the weekend a story that apparently has been circulating here in Washington. I did not see the actual broadcast, but this has to do with, I believe, something that ran on your network on the news and had to do with the Soviet ship that was in a port in Nicaragua.

And it is my understanding that the source of the film was a Cuban source, yet your network did not tell the viewers that fact, and they were told that it was a source friendly to Nicaragua.

First, I would like for you to comment and tell me if that is true. If it is true, how do you justify that, when everything I have seen for the last 10 days, or at least for the first few days of the invasion, had stamped all over it on every network that I saw that the source was the Pentagon or U.S. Government or U.S. military?

Mr. JOYCE. That was, indeed, a ship that Mr. Reagan had mentioned at a news conference or a—I believe it was a press conference. One of our people in Central America learned that film was available from a free-lance crew. There were Cubans as part of that crew, and, indeed, it was clearly labeled in an attempt to help viewers understand the nature of the film, that this was a source friendly to Nicaragua, an attempt to clearly identify it as material that you might choose to be skeptical about.

Mr. KASTENMEIER. The time of the gentleman has expired.

Mr. DEWINE. But if I could have just one followup, with the chairman's permission?

My understanding of your testimony today then is that it was not from the Cuban Government; the source was not the Cuban Government?

Mr. JOYCE. That is correct. That is my understanding.

Mr. DEWINE. That is your understanding?

Mr. JOYCE. Yes.

Mr. DEWINE. OK, thank you.

Mr. KASTENMEIER. I would like to now call on the gentlewoman from Colorado, Mrs. Schroeder.

Mrs. SCHROEDER. Thank you very much, Mr. Chairman, and I thank the distinguished panel for being here.

First of all, Mr. Chairman, I would like to ask unanimous consent to insert into the record William Safire's article "Us Against Them" that was in the New York Times on Sunday, October 30. It delineates a lot of the other things that have been going on in the attempt to control information coming out of the Government—the lie detectors and all other sorts of things.

I chair the Civil Service Committee. We had intensive hearings on this and found that the main source of leaks were White House political appointees and not, A, the press or, B, bureaucrats or, C, others.

So it is very important to put this in.

Mr. KASTENMEIER. Without objection, that will be received into the record.

[Committee insert:]

[From the New York Times, Sunday, Oct. 30, 1983]

ESSAY: US AGAINST THEM

(By William Safire)

WASHINGTON, Oct. 29.—The same vicious virus that infected the Nixon White House and caused its ruin is now raging through the Reagan Administration.

"The press is the enemy," Mr. Nixon used to say. That contempt and hatred for an unelected elite led to the bunker mentality of "Us Against Them," and then to an obsession with leaks and the excesses of Watergate. The same baleful mood permeates the White House and the Pentagon today.

But this President skillfully masks his animosity toward reporters; he limits to private counsels his denunciation of his earliest journalistic supporters as "hostile." Not merely "critical"—the word the President uses is "hostile": They have crossed over to the enemy, to "Them."

To defeat "Them," he has directed a campaign now reaching crescendo:

1. *Lie Detectors.*—To frighten government officials away from reporters, Mr. Reagan signed an order making it possible for a bureaucrat to demand that his employees take polygraph tests whether or not leaks have taken place or the employees are under suspicion. Asked if the Administration would administer these random tests, Attorney General William French Smith replied, "Why on earth would it do that?" But while the head of the Justice Department professed ignorance, Deputy Assistant Attorney General Richard Willard, 35, the John Dean of the Reagan Administration, curried favor in the Oval Office by testifying to the contrary.

2. *Memoir Censorship.*—Mr. Reagan has ordered that all government officials be required to sign lifetime agreements to submit future writings for Government clearance. This attempted rape of the First Amendment would force all outgoing officeholders to plead with their replacements to allow the publication of memoirs or informed criticism of the new administration's policies. Under this rule, if President Reagan did not like President Carter's book he could have suppressed it. The White House counsel stands inexcusably mute.

3. *Control of questions.*—In seeking to gut the Freedom of Information Act, in requiring all White House officials to report to a central authority before returning calls from reporters, and in undermining the tradition of regular press conferences, this President has made a policy of avoiding questions that might show him out of touch. Not since Watergate in 1974 has a healthy President avoided reporters for as long as Mr. Reagan did this fall.

4. *Blackout of War News.*—Fearful of television pictures of casualties and impressed by Mrs. Thatcher's management of a supine British press during what I will now call the Melvinas war, the President dictated that coverage of his Grenada invasion would be handled exclusively by Pentagon press agents. He not only barred the traditional access, but in effect kidnapped and whisked away the American reporters on the scene.

The excuse given for this communications power grab were false. Casper Weinberger, with an inarticulate martinet at his side, pretended that reporting was

denied because of concern for journalists' safety, which is absurd: The Reagan Administration would hail the obliteration of the press corps. Another reason advanced—that the military was too busy to provide the press with tender, loving care—is an insult calculated to enrage journalists.

The nastiest reason, bruited about within the Reagan bunker, is that even a small press pool would have blabbed and cost American lives. Not only is this below the belt, but beside the point: We know that the Cubans knew of the invasion plans at least a day in advance. In fact, the absence of U.S. war correspondents has curtailed criticism that the Pentagon miscalculated and sent in a dangerously small initial invasion force. The C.I.A. should have had a team with a radio on that island a week before the landing.

What has caused the Reagan men to invite a war with the press in the midst of two military campaigns? I should be writing today of the strategic importance of this timely invasion, which I favor and applaud; and here I am looking at my old friend Cap Weinberger with dismay. He is an intelligent human being, a good man, a patriot; and now he is declaring a willingness to obstruct military justice by ruling out a court-martial in Lebanon; professing his abdication of control of the military on press coverage, which is a matter of public policy, and—in my sorrowful opinion—lying through tight lips about why he barred the press from the battlefield in Grenada.

Perhaps Cap is driven by a desire to reaffirm membership in Mr. Reagan's Us. Since the press hates Us, he can indulge in the politically popular hatred and harassment of Them.

Count me among Them. I wish my former colleagues now in the bunker would remember Mr. Nixon's words in his farewell: "Those who hate you don't win unless you hate them—and then you destroyed yourself."

Mrs. SCHROEDER. Let me then build a little bit upon this because what Safire is intimating is that this administration is carrying on Nixon's war against the press. That is, you do something terribly popular, you control the news coming out, and then you unleash your guns on the press.

I think all of you must be aware that your being here this morning puts you in a very difficult position. Do you feel that you are kind of losing the war at the moment with the American population on this issue?

Mr. CHANCELLOR. Well, I will start the responses. I think we are losing the war, and we are in danger, I think, of losing the whole business, but it seems to me, Congresswoman, it goes beyond the press versus the Reagan administration, and I would like to speak to that.

In the last year or two we have seen three of the world's most notable democracies bottle up information going to their people.

The Israelis, one of the world's most respected democracies, in their invasion of Lebanon, used political censorship early in that conflict.

The British, the mother of Parliaments, used political censorship and actually deliberately misled its own pool reporters, the British reporters, in the invasion of the Falklands. That was censorship.

And now we find in a major and historic moment in American history the press was denied access when it was most needed by the United States.

So it is not a question of our complaining about President Reagan and his men. I think the press all around the civilized world has a problem when our beloved democracies are beginning to impose censorship on us.

Mrs. SCHROEDER. And the response to that is going to be that, well, the Russians do it, and after doing it they appear to be winning, the world must have changed.

Now, how do you respond to that, I think what is going on in the American mindset, is that, look, we didn't let the press there. They are all yelling about it, but this is one we won, and maybe we shouldn't ever let them in because that is how we win?

Mr. CHANCELLOR. Well, that is certainly a point of view that any bureaucrat would subscribe to. We know that. I mean, the press is one of those—it is kind of the vermiform appendix of democracy, you know, but yet I think it is a very important thing to have.

Most governments would like to exist without the press, and I think it is the role of the Congress in the United States, of Parliament in Britain, of the Knesset in Israel to fight against this on behalf of the press.

We can complain, but I think, as Congressman Moorhead rightly pointed out, a survey was 2 to 1 against us, and I think my mail is running 8 or 10 to 1 against the positions I have taken.

Mr. JOYCE. Congresswoman, if I might respond.

If the events of the past few days had not taken place, I would today be at Warwick Castle in London taking part in a seminar with a number of representatives of the press from around the world and a number of world leaders, and the subject, ironically, was to be, and still will be without my presence, media and the coverage of war.

And as I began to prepare for that, I thought, truly, the difference between the American and the British system, particularly with their experience in the Falklands, will emerge, and I must say I felt rather smug because ours is a country founded by people who realized from their own bitter experience that if the crown could control the monopoly of information, maintain a hold on the information flow to the Nation then freedom would always be at peril, and they were determined to give us a society where that would not be the case, and it seems to me that is a very precious heritage, one we need to treasure and one we need to protect.

And I have thought frequently over the past few days that if I were able to take part in that seminar in Great Britain I would hardly feel as smug.

Mrs. SCHROEDER. I totally agree with you, but I think the thing I am so distressed about is it has been tarnished, and I think Mr. Chancellor so eloquently said it isn't just this administration, every politician, everybody would like to control the press.

But the appearance now worldwide has been the way you win is by controlling the press. So those of us who believe in the first amendment and the Jeffersonian principles and think it is so essential are now on the defensive.

Mr. JOYCE. Well, it seems to—

Mr. KASTENMEIER. I am sorry, the time of the gentlewoman has expired.

Did you wish to—

Mr. JOYCE. I just wanted to say that it seems to me that there are not only disturbing implications domestically, but as someone who runs a worldwide news gathering organization, I do have concerns about our people overseas who, dealing in some very difficult parts of the world, have been able to say we are the American press and this is the way we do business. I am worried they will have a more difficult time in the future.

Mr. KASTENMEIER. Now, I would like to call on the gentleman from Michigan, Mr. Sawyer.

Mr. SAWYER. Thank you, Mr. Chairman.

Well, having listened to Mr. Chancellor's diatribe on Monday night, I am delighted to hear that your mail is running 8 to 1 against you. [Laughter.]

Now, I am not a letterwriter, but I came awfully close to writing one on that, and it is refreshing that the public responds well.

We didn't have any media along on the Iranian rescue attempt, did we?

Mr. CHANCELLOR. No, sir; but the fact is that the press did not complain that it wasn't asked on that mission. That is a very key point.

Mr. SAWYER. Well, that was a rescue mission, wasn't it?

Mr. CHANCELLOR. That is right.

Mr. SAWYER. And that is what the administration says that this was as far as the students were concerned. I mean, you maybe disagree with that, but that was their position on it, as I understand it.

Mr. BRINKLEY. Well, the Iranian rescue attempt was very small and very brief. It was all over in a few hours.

Mr. SAWYER. Well, that is because it was bungled.

Mr. BRINKLEY. Well, OK.

Mr. SAWYER. It may have been quite an extended operation if it had not run into the disaster.

Mr. BRINKLEY. But it was still small.

Mr. JOYCE. I don't think, sir, with all respect, it was projected as an extended mission. I don't think there was any thought of holding Tehran or holding a section of Tehran.

Mr. SAWYER. Is it the size that governs then whether the media ought to be present or not?

Mr. JOYCE. Well, I think, sir, while you were out of the room on other business we—

Mr. SAWYER. I was out of the room to vote. There was a vote on on the floor.

Mr. JOYCE. Yes, sir; I understand that.

I think a number of us did make the point that none of us sitting here today is saying that there cannot be secrecy, that we object to a concept of military secrecy.

Mr. SAWYER. But where is the size cutoff? I mean, how big a group, before all of a sudden, you need the media, and how small a one so that you don't need them?

Mr. BRINKLEY. I don't think it is a question of size, Congressman.

Mr. SAWYER. Well, I thought that was the point somebody made, that the Iranian thing was small.

Mr. JOYCE. Small and of short duration.

Mr. BRINKLEY. We did, we did. It was a small operation.

Mr. SAWYER. Well, it was of short duration. This could have been of short duration, too, if it had been a disaster, I presume.

Did the Israeli—or did any press cover Entebbe?

Mr. BRINKLEY. I don't think so.

Mr. CHANCELLOR. No, sir; but the point is, Congressman, that if Israel had used 15,000 troops to rescue their nationals at Entebbe and had stayed on to occupy parts of the country, I can guarantee

you that there would have been at least a pool, and a sizeable pool, of the Israeli press along with those 15,000 Israelis.

Mr. SAWYER. Well, then you do fix a size cutoff somewhere then. Where do you fix it?

Mr. ABRAMS. Congressman, I think it is size and duration of the operation, too.

Mr. SAWYER. Oh, both size and duration?

Mr. ABRAMS. Yes, and if the Israelis were taking Uganda, throwing out the government there, and installing their own government, it might have been a different case.

Mr. SAWYER. Actually, didn't—and maybe a far more important episode in the world picture—didn't Kissinger go totally unbeknownst to Beijing and open the gateway to the Chinese Government without the press having any idea of where he even was, thinking he was somewhere different?

Mr. BRINKLEY. Yes. Yes, he did, but it was not a military mission.

Mr. SAWYER. Well, then is a mission that opens up communications between China and the West of less press moment or world moment, news moment, than the invasion of a little island in the Caribbean? Is that your view?

Mr. BRINKLEY. Probably not, but it was not a military mission. It was a visit by a diplomat to a capital with which at that time we had no diplomatic relations, in secrecy, and was rather brief, and as soon as it was over we were told all about it.

Mr. SAWYER. Well, I yield back, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from Connecticut, Mr. Morrison.

Mr. MORRISON. Thank you, Mr. Chairman.

I would like to focus just for a minute on your perceptions about the degree to which we were denied an accurate picture of what went on in Grenada by the exclusion of the press, beyond the principle, from the information that is available to you now, that there has been some limited amount of access.

Any one of you that would like to comment on that?

Mr. BRINKLEY. Ed, why don't you do that?

Mr. JOYCE. Is your question pointing toward unanswered questions which remain unanswered, or is it—

Mr. MORRISON. Well, unanswered questions and conflicts that you see between what you can now determine but that has been lost to the American people in having an accurate picture by the lack of access.

Mr. JOYCE. Well, there are a number of unanswered questions, some of them I mentioned a moment ago when I suspect you were outside the chamber voting.

What about the Americans who have remained on the island and refused evacuation? What did they have to say during those early days?

The performance of American military forces. I mentioned that there is no independent verification.

The nature of the bombing of the hospital. We had on CBS news last night the director of the hospital, who said very clearly, in his opinion, this was not the fault of the American military forces. It

was the fault of the People's Militia of Grenada who had occupied that building and had flown a flag.

It would have certainly been useful to have had reporters on the scene at that time.

Who fired first? The question has come up because the Cubans claim they gave specific instructions to their people not to fire. It would have been valuable to have had independent verification of that.

The nature of the Cuban opposition. The Grenadian Army. We have heard a great deal of that. There were more Grenadian than Cuban troops on the islands, and yet official dispatches depict the bulk of the resistance as coming from the Cubans.

Was the Russian Embassy fired on?

Getting back to the mental hospital, was enemy fire coming from that hospital?

All questions for which at this point we don't have answers. We might very well have had answers if an independent and free press had been operating on that island.

And the point I guess I am making is that history may never catch up to the answers to some of these questions.

Mr. MORRISON. Do you think there is any correlation between the overwhelming public approval, or apparent approval, of the operation and the lack of information from the press, independent information?

Mr. JOYCE. It is my impression at a time of military action there is almost always initial approval of that action. It is the nature of all of us Americans, who are very patriotic people.

Mr. MORRISON. Beyond the scrutiny that these hearings are focusing on this question, do you have any specific proposals of how Congress could constructively prevent a future occurrence like this?

Mr. JOYCE. Sitting here today, sir, I really don't come with answers to that. I came and welcomed the opportunity to appear before this subcommittee because of my great concern that this not become a 1-week issue that occurs, that is forgotten, and that the military looks at as an example of a future technique they can use over and over and over again or, indeed, that other arms of government say this is a terrific approach.

Mr. BRINKLEY. Mr. Morrison, it seems to me a legislative remedy to this would be extremely difficult.

Mr. Sawyer, for example, has asked what size military operation should the press be allowed to cover. Well, I don't think anybody could set any such standard.

I wish I had a better answer, but I don't. I don't know how to do it. I would not know how to do it legislatively if it were up to me.

Mr. MORRISON. Mr. Chancellor.

Mr. CHANCELLOR. Well, I have just asked Floyd Abrams, who knows more about the law than all the people in journalism put together, but I think that we have had—that the Government itself, the Government of the United States, has a great problem about censorship.

Censorship was an established method of controlling information that the press believed in and the Government believed in when people were writing with quill pens. It was a pretty effective way of

controlling security for the Government when we were just laying cables across the Atlantic for telephone calls and cablegrams. But today, with ground stations and satellites and instant communication all over the world, I think we have to think censorship out all over again and see if the press and the Government can behave responsibly toward one another in this.

And so, I would welcome anything that the Congress could do, and I would welcome, more than that, an agreement in some form—I don't know if it could be legal—in some form between the national press and the U.S. Government on how these things ought to be arranged because if we can't do that with fairness to both sides we are going to have this kind of trouble again.

Mr. MORRISON. Thank you, Mr. Chairman.

Mr. KASTENMEIER. Yes. Actually, Mr. Morrison raised the question that I would have raised. I suspected the answer would be that there would be no particular recommendation, and I agree with you that it would be extraordinarily difficult to formulate a legislative solution.

We have devoted a great deal of time to the question of newsmen's privilege nationally. In the final analysis, the journalism societies and the publishers said do nothing because it would require a definition of who is a reporter. And rather than federally start putting all those things into some law which would discriminate against some and qualify others, it was decided that legislation was not the answer.

I suspect it is the case here. The vigilance will have to come from people who believe in the first amendment, who believe in sticking up for the press, to make a public issue of it; but I sense that there is no easy legislative resolution for it.

However, if anyone sees a course of action that does involve one, we would very much like to know what it is.

Mr. ABRAMS, perhaps you might comment further.

Mr. ABRAMS. Congressman Kastenmeier, I think what you are doing today is the best thing you could do. I think the idea of having hearings, the idea of talking about these things, and trying to get people to focus on them on one side or another is about the best beginning.

I don't see any legislative resolution of this at all. I think, in part, it is a matter of mindset, and that can be changed by persuasion. I don't think this administration was doing this to get the press. Russell Baker had an amusing column, suggesting that the Grenada invasion was an effort to teach the press a lesson, but he was at least four-fifths kidding about it.

I think that all we can start with is talking about it and exchanging views and hoping that in the end people of any administration will understand and will accommodate the first amendment needs, not just of the press, but of the public.

Mr. KASTENMEIER. Are there further questions?

The gentleman from California, Mr. Moorhead.

Mr. MOORHEAD. I think that what we are up against is a question of judgment, from your answers, and I think, Mr. Brinkley, you had an outstanding answer that I certainly agree with, when you say that you can't just judge by size. It depends upon all the cir-

cumstances that surround a situation, and any administration has to make a judgment.

The more people you let in on a decision or a surprise attack, the more chances there are of leaks, and I don't think the press is any more suspect than any other element in our society, including members of Congress. But the more people involved, the more chances there are of leaks.

The administration made a judgment to protect their soldiers and their sailors, and I think it is our right to now examine that decision. Maybe they didn't let the press in soon enough or maybe they let it in just at exactly the right time.

But I don't think that we as Americans should consider any one group, regardless of where they come down on that kind of a judgment, as wanting to cut back on the democracy in this country or the freedom of information for the American people because I, as a member of the minority, would fight for that sooner than almost anyone.

We survive because the press is free and can print the positions of both the Government and those that are not in control. So it is most important.

I just think in this case the administration came down on a position. They felt that it was in the best interest of those soldiers and marines that were going over there, and that is why they took the position they did.

I think that it is fine for you to say that the press should have been allowed in sooner, and in these discussions we can best find the right answers for the next time this type of event comes around.

I would like your comments on that.

Mr. BRINKLEY. Well, I would not disagree, Congressman. My view is that we should have been allowed to go into Grenada much sooner. It was more than 1 week.

During that week there was a proliferation of rumors and stories coming from all sorts of places because we were in no position to verify any of them.

I will give you a specific example. About 1 week ago, I had a guest on television named Caldwell Taylor, who was the last Ambassador of Grenada to the United Nations, and I said to him, "We hear there are all sorts of weapons and heavy rockets and this and that being found in your country. Why were they there? What did you have in mind doing with them?"

He denied they were there. He said it was lies by the American military, which, of course, I do not accept and did not believe, but was in no position to argue because we had no one there. All we knew was what we had heard secondhanded from the Defense Department—and again I don't accuse them of lying. I would not do that.

But we had no independent information of our own with which we could refute Taylor's—I am sure it was a lie he was telling. But in any case, he said he didn't believe they were there, and if so they had been brought in by the marines and planted, and so on.

Stories like that, which are very disruptive, spread rapidly when there is no source for verification, as in this case.

Mr. JOYCE. Congressman Moorhead, first of all expressing gratitude for your gracious and openminded examination on this subject, let me submit that it appears that this invasion was not a secret to the Soviets, not a secret to the Cubans, who knew that it was on its way. It was a secret to the American people.

But even accepting the premise that initial secrecy was a good idea, was required, there was obviously some threshold that got crossed very early on in which we move from military to political censorship, and I think that is something that is worthy of discussion and, with total respect, worthy of some concern on all our part.

Mr. MOORHEAD. You know, there is no question that there was a leak in Guyana in which the press did report the possibility of an invasion because they had been in on the little group of countries down there that had been talking about what was going to happen. But obviously, it wasn't taken seriously by the Cubans because all of the secret papers and everything else were found intact in Grenada.

The commanders hadn't gotten to their troops. They weren't organized, and there was secrecy regardless of the fact that this story had been printed in obscure newspapers of this little country a day or two before.

So really, there was secrecy even though there had been a leak, and I think that is an important point.

Mr. JOYCE. Sir, but would you agree that within hours of that invasion the secrecy justification had evaporated?

Mr. MOORHEAD. I really don't know enough detailed facts to give you an answer to that question.

Mr. CHANCELLOR. Congressman, may I just interject here that I don't think probably any of us in this room know all those detailed facts, and I certainly don't think we should get into a debate on the Grenada situation until we have learned a little more about it.

I think personally that the press was held far too long, but let me suggest to you, sir, that what we are talking about is the future. If the American Government can do this to the American people through its press in Grenada, maybe another administration, a Democratic administration, can come along and do the same thing again in another part of the world.

What I think we all have to address ourselves to is some plan under which we can have a small pool of, say, 20 people from the press, camera people, and reporters, that is all, that can be secretly transported to the scene of a major involvement by the American military, and be there with them taking the risks, as we always have done.

It seems to me this Republic could stand something like that.

Mr. MOORHEAD. Well, I certainly wouldn't object to that program. I think this operation came up so fast that there wasn't time to do that.

Mr. KASTENMEIER. The time of the gentleman has expired.

I would hope we wouldn't need that pool very often, although one doesn't know.

Is the gentleman from Ohio seeking recognition?

Mr. DEWINE. Yes, very briefly, Mr. Chairman.

It seems to me that our testimony today, gentlemen, has brought out how tough these decisions are, that they are factual decisions, that they vary from case to case, and I very much appreciate your input and your testimony here.

It just seems to me that, as I stated before, what we are dealing with is a very tough balancing decision between access and the safety of either hostages or the safety of American troops who are going in. These decisions, I think, have to be made on a case-by-case basis, and I think our discussion today has been illuminating, and I think it will help those decisions that are made in the future.

I do have one question, and I don't think this has been brought out. We have been talking about when you had access, and there has been some statements about 5 days, 6 days, a week.

I have some figures, and I just want your comments to see if they are, at least in your understanding, correct as far as when the media had access.

It is my understanding that on the third day there were 15 journalists in a pool who were in for a brief period of time. The fourth day there were 27. The fifth day, 47. The sixth day, 172. And the seventh day, 197.

Now, I don't expect you to respond that those are accurate or inaccurate, but is that roughly correct? Is that a fair representation of your access to the island?

Mr. JOYCE. Yes, sir, it is my understanding that that is generally correct.

If I may point out, that as you describe that third day, what happened was that three network correspondents were allowed on the island with a pool crew.

It needs to be pointed out, however, that their tour, if I might call that—it was, indeed, a guided tour of a limited part of the island—did not represent the sort of access that in other battlefield conditions reporters have had in the past.

Mr. DEWINE. Thank you, Mr. Chairman.

Mr. SAWYER. Mr. Chairman?

Mr. KASTENMEIER. The gentleman from Michigan.

Mr. SAWYER. Yes. Just further reference to that third day, it was my understanding that that group representing the three networks were supposed to act as a pool and share the information with other media, and then they didn't do it.

Mr. JOYCE. That is not my understanding, sir.

Mr. BRINKLEY. Not to my knowledge. Does anyone know more about that than I do?

Mr. CHANCELLOR. There was a report, Congressman, that—I am not sure it involved people from television. I do not say that defensively. I think it involved some of the people who were from the newspapers or the wire services, who came back and in conditions of absolute chaos, back in Barbados, as far as communications were concerned, either did not fully brief or did not at all brief their colleagues.

The problem was that when the people were actually brought back from Grenada to Barbados, there being no facilities made for press communication on Grenada, they found only a dozen telephones installed, and when the reporters came back they found all connections out of the island, Barbados, were jammed for hours.

The communications, frankly, has been a disgrace, and it is one thing to take in a small pool of reporters into a combat situation, but if they come back and nobody can file because there aren't enough telephones, and the military—any political campaign will tell you how to put in telephones—if those telephones aren't installed and you have got a terrible jam-up at the press center, then that in itself delays and impedes the free flow of information.

Mr. SAWYER. Just one other observation. Mr. Brinkley made the statement that no one was in there for a week. That is somewhat of an exaggeration. Only the first 2 days were there no press there, and then this pool came in on the third day, and then by the time a week was up, there were 197 journalists on the island, with the amount growing.

So, you know, it is a pretty good story without making it better.

Mr. BRINKLEY. Well, if I said no one was in there for a week, obviously I was not correct.

It was about a week before anyone was allowed to go in and circulate freely and do whatever he thought he should do.

Mr. SAWYER. Well, on the fifth day there were 47, on the sixth day 172.

Were they all just shepherded?

Mr. BRINKLEY. Essentially, those are guided tours, Congressman, taking them to limited places for limited times, and then flown back to Barbados.

Mr. SAWYER. Thank you. I yield back, Mr. Chairman.

Mr. KASTENMEIER. If there are no further questions—the gentleman from Colorado.

Mrs. SCHROEDER. Mr. Chairman, I wanted to ask a couple more questions trying to hit on the reasons for why this was supposed to have happened.

Are any of you aware of any time that the press ever revealed this type of information if they had it ahead of time?

In other words, part of the reason for not letting you in was supposedly to maintain the secrecy.

Has there ever been documented a case where the press was in on something and it was revealed?

Mr. CHANCELLOR. In a book recently published by Colonel Harry—written by an officer named Col. Harry Summers, who teaches at the Army War College, there was not a single incident of a tactical operation in the course of the Vietnam war where security was broken by the American press. That is a book that came out, I think, just last year.

I will give one example of the ability of the press to keep secrets, and that is that before the American hostages were released in Iran, before the American hostages there were released a number of us in the press knew that some Americans had escaped early in that ordeal and were being sheltered in a Western embassy in Tehran. We knew that, and not a word of it appeared in the American press or on American television or radio.

It was a very well-kept secret for a very obvious reason. It would have endangered lives. It was a very good and dramatic and interesting story, and we later learned about it when they were released by the Canadian Embassy. But that was known by the major news

organizations in the United States, and not a word of it got into public.

Mrs. SCHROEDER. So it would be fair to characterize it that no one is aware of any documentation of secrecy being broken on that type of thing?

Mr. BRINKLEY. None that I know of, Congresswoman.

Mr. JOYCE. That is my understanding.

Mrs. SCHROEDER. My next question concerns the security of the newspeople. I guess what I want to know is what do you demand from the military when you are going in. Suppose you had been notified ahead of time, and they were going to let you in, and assuming you kept the secret. What would you demand? Would you demand extra ships or planes for your cameras? Do they do it at their expense or your expense? What do you require?

It almost sounds like a day care operation from the way they are trying to characterize it. Is that what it is? Do you require special troops to protect you?

Mr. BRINKLEY. The only services we, in these circumstances, require of the military are those we are physically or otherwise unable to provide for ourselves. Everything possible is done at our expense, not theirs.

When, in the case of Grenada, there is no commercial air service and no boats are available, the only way to get there is with military help. If they want to charge us for it, fine. We are happy to pay it. We are looking for no handouts.

Mrs. SCHROEDER. Mr. Joyce, would you pay the bill if they charge you?

Mr. JOYCE. Of course we would. Indeed, we pay our share of Air Force One when the press uses Air Force One.

We had literally minutes away from Grenada a sizable contingent of our people on Barbados. We would have—

Mrs. SCHROEDER. And they paid to get there on their own?

Mr. JOYCE. Yes, they did.

If the military had been unable to fly them in, we, with a charter airplane, would have taken them in. We would have taken them in by boat. We have reporters who would have paddled to get there.

Mrs. SCHROEDER. Would you have made them stop and put phones in for you on Grenada?

Mr. JOYCE. Phones? If they can do that, fine. I don't think we need to place the burden on the military to provide facilities for us. We ought to be in the business of providing our own facilities.

Mrs. SCHROEDER. Has anybody in the press ever sued the military for not providing adequate protection? Do they ask to be protected personally? Is it like secret service?

Mr. BRINKLEY. No way. No one in the press has ever sued the military. I have never heard of such a thing.

Mr. JOYCE. No.

Mrs. SCHROEDER. So actually asking for personal security is not something you do? You figure you were there—

Mr. CHANCELLOR. Congresswoman, you sign a waiver when you go into a combat zone if you are going in with the troops of any government, and this is standard operating procedure all over the world, and, indeed, on just about every police press pass that reporters carry it says somewhere on there that you absolve that

police department from any responsibility for injuries you may have while you are behind their lines, and that applies to the military, and it applies in every combat situation.

We waive our rights automatically, and they are taken up by our own news organizations.

Mr. JOYCE. Each of us represents news organizations who have lost people in battle, and the military has never had that kind of a problem.

Mrs. SCHROEDER. You as the corporation carry life insurance or whatever?

Mr. JOYCE. We do, indeed.

Mrs. SCHROEDER. And so that is how you pick it up?

Mr. JOYCE. And we carry special casualty insurance for people who do that line of work.

Mrs. SCHROEDER. And lastly on the Government action question that a prior Congressman asked about, there are some things we could do about the prior restraint things and the lie detector things, I think, that we could pass in the House, probably not in re Grenada itself, but—

Mr. ABRAMS. Yes, Congresswoman, I think there are lots of things you could do. You could emulate what the Senate did and have a rider on the appropriations bill, and that would have some real immediate, genuine, and lasting effect.

Mrs. SCHROEDER. Thank you, Mr. Chairman.

Mr. KASTENMEIER. Does the gentleman from Kentucky have any questions?

I wish to acknowledge his presence.

I have just one question of Mr. Abrams; that is, we have heard a great deal this morning about the experience, information problem.

Can you relate this in terms of a larger experience and whether or not you see this as any part of the pattern or should we see it only as an isolated event?

Mr. ABRAMS. I have two observations, Congressman. First, I think we have to recognize the uniqueness of this country in terms of our dedication to an open society and to information being made available to the public generally. Not only are we different from the states that don't share our dedication to a free society, but we are different from Western European states in the degree of our dedication to first amendment principles, to use the shorthand word.

That being said, I do see this as part of a broader pattern of behavior. It is my view that in a series of events in recent years—an article that I wrote in the New York Times did deal with the Reagan administration—that when you look at the totality of behavior with respect to the changes in the classification system, changes which were proposed for the Freedom of Information Act, and the new secrecy agreement, and the use of the McCarran-Walter Act, and a variety of other things, that there has been a change, in my view, in governmental action, and that there has been a new mindset about this which is different in quality and nature than has existed before.

We have had administrations before which have, in my view at least, misused the McCarran Act, and in my view at least, proposed legislation inconsistent with the first amendment, but I don't recall

one which has so consistently acted in a fashion inconsistent with the public right to information and which has a policy which one can talk about in so many areas which are inconsistent with that right and with that need.

And so I do, for myself, view the episode with respect to Grenada as part of a larger discernible pattern of behavior and thinking.

Mr. KASTENMEIER. Thank you, Mr. Abrams. I want to thank the panel and the committee—

Mr. MORRISON. Mr. Chairman, would the chairman yield for just a question to the chairman?

Mr. KASTENMEIER. Yes.

Mr. MORRISON. I think that the information from this panel has been very helpful, but I am concerned that at the moment on our schedule we don't have appearances by anyone in the administration, particularly the Secretary of Defense or others, who made the decisions about the Grenada coverage, and frankly, I find what we hear from the news organizations to be quite persuasive on the point that persuades me that there are a lot of questions that ought to be directed back at the Secretary of Defense and others, and I would hope we might include that in short order.

Mr. KASTENMEIER. The gentleman's inquiry is very timely. I would like to take that matter up with my colleagues, Mr. Moorhead and others, and if we can agree on other witnesses on this and other subjects who would perhaps present a different perspective, that would be fine.

Mr. MORRISON. Thank you, Mr. Chairman.

Mr. KASTENMEIER. We will work with the minority on that.

I would like to thank you, Mr. Joyce, Mr. Chancellor, Mr. Brinkley, and Mr. Abrams, for your contributions today. The committee is indebted to you.

Thank you very much.

We have one other panel today. Originally we had hoped for three panels. We had hoped that Mr. Harrison E. Salisbury could come, however, he was not able to be here.

We do have two individuals, Mr. Ralph W. McGehee, who is the author of a book entitled "Deadly Deceits"; and Mr. James Bamford, author of "The Puzzle Palace."

Mr. Bamford holds a law degree and is a writer and lecturer. Both have had extensive experience with national security agencies; in Mr. Bamford's case, the National Security Agency, and in Mr. McGehee's case, the Central Intelligence Agency. Mr. McGehee has challenged the classification censorship system in a suit which was recently decided by the court of appeals for the district circuit in favor of the Central Intelligence Agency.

Both of these gentlemen have personal experience with Government policies, and we are pleased to have them here.

Mr. Bamford, would you proceed with your statement?

TESTIMONY OF JAMES BAMFORD, AUTHOR OF "THE PUZZLE PALACE"; AND RALPH W. McGEHEE, FORMER CIA OFFICER, AUTHOR OF "DEADLY DECEITS"

Mr. BAMFORD. Thank you, Mr. Chairman.

Mr. Chairman, I welcome your invitation to address the committee today on the issue of Government restrictions on access to information and, in particular, on how these restrictions have affected the publication of my recent book on the National Security Agency, "The Puzzle Palace."

"The Puzzle Palace" may be the only book in history to have been totally unclassified as it was being written, yet top secret by the time it was published. And the reason for this "Alice in Wonderland" situation is the little known yet potentially sinister policy of reclassification.

The recent actions which the NSA took, which I shall discuss below, are best understood when one considers the Agency's historical obsession with secrecy. Unlike the CIA, which was formed openly through Congress with the passage of the National Security Act of 1947, the NSA was formed in total secrecy by a seven-page Presidential memorandum signed by Harry Truman in 1952 and which even today is still top secret.

For much of NSA's first decade, its very name and its very existence was considered classified information. It was only revealed in 1958 as a result of a spy scandal.

Shortly after the NSA became publicly known, NSA officials succeeded in slipping through Congress an extraordinary provision which permits the Agency to nearly deny its own existence and today makes it virtually immune from the Freedom of Information Act.

This little known subsection of an obscure NSA employment authorization bill, Public Law 86-36, provides:

Nothing in this act or any other law shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency.

Just to briefly give you a description of the actions that the NSA took, in terms of my book, first of all, I had never worked for NSA. I am an independent writer. I basically a writer with a law degree who does research.

The first action that the NSA took, took place when I was doing research for the book. I submitted a Freedom of Information Act request to the Justice Department for some documents dealing with illegal NSA activities. This was under the Carter administration that I requested the material.

The material, after a 10-month review, was released to me, yet 2 years later, once the Reagan administration came into office, they demanded that I give these very same documents back to the Government.

I refused to give the documents back to the Government and, as a result, had several meetings in Washington and Boston with NSA and Justice Department officials. At one point they threatened to use the espionage statute against me if I continued to refuse to return the documents.

Again, these were documents that the previous administration saw fit, after 10 months of review, to release.

I continued to refuse to give the documents back to the Government and used the documents in my book. The end result was that the Reagan administration changed the law. The law originally

said once a document had been declassified it can't be reclassified. Well, the Reagan administration, in April of 1982, changed the law to say once a document has been declassified it can be reclassified.

Mr. SAWYER. Mr. Chairman, could I just interrupt for a question?

Mr. KASTENMEIER. Yes; sure.

Mr. SAWYER. When you say the Reagan administration changed the law, how did they change the law?

Mr. BAMFORD. I am sorry. They actually changed the Executive order. They didn't change the law. They changed the Executive order.

Mr. SAWYER. Thank you. I yield back.

Mr. KASTENMEIER. Fine.

Mr. BAMFORD. The second instance took place actually after the book came out. What happened was that the NSA had never had a chance to review the book beforehand, since I never was under any obligation to submit the book to NSA for review.

Well, once they obtained a copy of the book they used the footnotes in the back of the book, and they went to one of the libraries which I had used extensively for documents. It was the George C. Marshall Research Library in Virginia.

They went down to the library and, again using the footnotes in my book, they began pulling off documents and papers that I had quoted from, from the library, from actually the shelves of the library, and began stamping those documents secret and ordering that the documents be locked into a vault.

Again, this was the first time the Government had ever done something of this nature, and it was done under the theory of reclassification.

The incident at the George C. Marshall Library was rather bizarre, since the information that they were pulling off the shelves and stamping secret was already quoted in more than 150,000 copies of my book, and it was material that had for almost two or three decades remained unclassified on the library shelves.

Just to conclude, I think that one of the most frightening aspects of the Reagan administration's war on words is the policy of reclassification. It would be total anarchy for historians and scholars who frequently spend years doing their research that if one administration would be permitted to recall history by forcing these people to return materials released by a previous administration.

About 350 years ago, Cardinal de Richelieu declared the principle under which the Reagan administration today is operating, and that is, "Secrecy is the first essential in the affairs of state." I think that is a sad commentary.

[The complete statement follows:]

PREPARED STATEMENT OF JAMES BAMFORD

Mr. Chairman, I welcome your invitation to address the committee today on the issue of government restrictions on access to information and, in particular, how these restrictions have affected the publication of my recent book on the National Security Agency, The Puzzle Palace.

The Puzzle Palace may be the only book in history to have been totally unclassified as it was being written, yet top secret by the time it was published. The reason for this Alice-in-Wonderland situation is the little known yet potentially sinister policy of reclassification.

The recent actions of the NSA, which I discuss below, are best understood when one considers the agency's historical obsession with secrecy. Unlike the CIA, which was formed openly through Congress with the passage of the National Security Act of 1947, the NSA was created in total secrecy by a 7-page Presidential memorandum signed by Harry Truman in 1952 and which even today is still top secret. For much of its first decade the existence and very name of the agency were considered classified information and known to only a few senior officials. A spy scandal in 1958 finally brought the agency's existence to light but its true functions were hidden under a bland cover story.

Shortly after the NSA became publicly known, agency officials succeeded in slipping through Congress an extraordinary provision which permits the agency to nearly deny its own existence—and today makes it virtually immune from the Freedom of Information Act. This little known subsection of an obscure NSA employment authorization bill, Public Law 86-36 section 6(a), provides: "Nothing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, or any information with respect to the activities thereof, or of the names, titles, salaries, or number of the persons employed by such agency."

Thus, under Public Law 86-36 the NSA may not only withhold classified information from the public, but even unclassified information if it so much as mentions the agency. This law has long been the envy of other U.S. intelligence agencies.

In the mid-1960s the NSA's obsession elevated to paranoia when officials discovered that David Kahn, an author, was about to include a chapter on the agency in his forthcoming book, *The Codebreakers*. According to the Senate Select Committee on Intelligence:

The Director suggested planting disparaging review of the author's work in the press, and such a review was actually drafted. Also discussed were: purchasing the copyright of the writing; hiring the author into the Government so that certain criminal statutes would apply if the work were published; undertaking clandestine service applications against the author, which apparently meant anything from physical surveillance to surreptitious entry; and more explicit consideration of conducting a surreptitious entry at the home of the author.

Although none of these measures were ever carried out, Kahn's name was placed on the NSA watch list thereby subjecting much of his communications to the agency's eavesdropping techniques. Also, the director of NSA secretly persuaded Macmillan, Kahn's publisher, to turn the manuscript over to the agency for review without the knowledge of the author.

The next serious attempt by an author to write about the agency was my book, *The Puzzle Palace*. In 1979 I entered into a contract with Houghton Mifflin to produce a well researched, heavily documented book on the history and activities of the NSA. Because of the lack of published sources on the subject, I was forced to depend primarily on Freedom of Information Act requests, publicly available records and documents, and interviews with current and former NSA officials. In all of these areas I proved considerably more successful than NSA would have liked. As a result, the Agency began a policy of classifying and reclassifying documents after I had already had access to them.

The first instance took place in late August 1980. Over the summer I had spent a number of days at the Naval Historical Center going over annual reports from various naval stations associated with the NSA. These reports were never classified. The usual procedure was to paperclip the items I was interested in having copied and they would later be mailed to my home. On August 29, 1980, however, the NSA discovered my research at the historical center and demanded that the center send to NSA the most recent materials I had requested. The NSA then stamped portions of the documents secret and returned the deleted versions to me. Nevertheless, I had taken notes from the now classified portions of the documents and therefore was able to include this information in my book.

The next instance of reclassification was considerably more serious. In September 1978, as I was exploring the possibility of writing a book on the NSA, I sent a Freedom of Information Act request to the Justice Department in an attempt to obtain information on a little known, highly secret criminal investigation into the NSA's domestic eavesdropping operations. At the Justice Department the request went to Robert L. Keuch, a deputy assistant attorney general in the Criminal Division. He determined that two documents, a task force report on the investigation and the prosecutive summary, came under the purview of my request.

Because of the classification of the documents, Top Secret Umbra, Keuch created his own task force to review similar materials already in the public domain and to base the declassification decision on that survey. He also decided not to submit the

documents to NSA or the CIA because the agencies were the principal subjects of the investigation and he felt that allowing them to review the reports would subvert the criminal justice system.

After 10 months, on July 5, 1979, Keuch released the requested documents to me, with some portions deleted.

Several months later the NSA became aware of Keuch's actions and requested that the Justice Department send it copies of the same documents. After a review, NSA Director Bobby R. Inman wrote to Attorney General Benjamin Civiletti, informing him that the documents contained still-top-secret information and that they should never have been released without first being sent to the NSA. Civiletti, believing that the documents had been properly declassified or else realizing that the executive order on classification forbade reclassifying documents released under the Freedom of Information Act, ignored Inman's protest.

Two years later, however, there was a new administration and a new attorney general and Inman's successor at NSA, Lieutenant General Lincoln D. Faurer, decided to try again. In a letter to Attorney General William French Smith, Faurer requested another copy of the two Justice Department documents. Copies were sent to both the NSA and the CIA and, as a result, the two agencies decided that portions on the documents should once again be stamped Top Secret. The fact that the 250 pages of documents had been in my possession for 2 years and, by then, were cited extensively in my manuscript, seemed to make little difference.

On July 8, 1981 the Justice Department contacted me and asked for a meeting to discuss the documents. At the meeting Gerald A. Schroeder, a senior attorney with the Office of Intelligence Policy and Review, explained that the Carter Administration had released the documents by mistake and asked me to return them. I indicated that I didn't think that that would be possible but that I would be willing to meet with him again to further discuss the issue. That meeting with Schroeder and two NSA officials took place in Boston at the offices of my publisher, Houghton Mifflin Co. This time however, when it appeared I was going to decline to return the documents, Schroeder brought up the possible use of 18 U.S.C. 793, the espionage statute. At that point, on the advice of my attorney, Mark H. Lynch, I left the meeting.

The following month I received a registered letter stating: "You are currently in possession of classified information, that requires protection against unauthorized disclosure * * *. Under the circumstances, I have no choice but to demand that you return the two documents * * *. Of course, you will have a continuing obligation not to publish or communicate the information."

In response, we simply cited section I-607 of the Executive order on Classification (EO 12065) which stated: "Classification may not be restored to documents already declassified and released to the public" under the Freedom of Information Act.

To overcome this, President Reagan on April 2, 1982, issued a new executive order on secrecy which now gives the President or any agency head the power to reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security, and (2) the information may reasonably be recovered. When questioned by the press as to the meaning of the term reasonably, the administration refused to rule out the use of surreptitious entry.

Because it would have been ex post facto, the Justice Department did not attempt to enforce the new order against me and the book was published on schedule, without any deletions, in September 1982. That fact, however, did not deter the NSA from their reclassification efforts.

Using the reference notes at the back of my book, the NSA launched what one official termed a systematic effort to track down and, if necessary, remove from public circulation research materials about sensitive matters that were quoted in the book. The chief target was the George C. Marshall Research Library, a private nonprofit library on the campus of the Virginia Military Institute in Lexington, VA.

The materials they were most interested in were the papers of William F. Friedman, one of the founders of American cryptology and considered by many the father of the NSA. He had retired from the NSA in 1955 and, over the years, became greatly alarmed at the NSA's increasing, almost fanatical attitude toward secrecy. "I had a couple of sessions yesterday with the guiding lights at [Fort] Meade," he once wrote to a friend, "and I find the scientific climate so devastating that I am heartsick. The root of the evil is that they have gone overboard on security."

As a result of his dismay over the NSA's attitude toward secrecy, Friedman vowed never to let the NSA get hold of his books and private papers. Thus, Friedman wrote to a long time friend:

Without doubt you will wonder: Why did I choose to bequeath our collection to the George C. Marshall Foundation? Why not NSA? Or the Library of Congress? Or some other government institution? As to NSA we know that the Collection would not be available to scholars and students there, because no one—but no one—without a high-degree clearance can even enter its portals. The Library of Congress would disperse the items—they don't have the funds to keep collections intact, and duplicates of items on their own shelves would be sold or given away to some other library in exchange for an item the L. of C. might lack. At any rate the Friedman Collection will be kept intact at the Marshall Foundation and available for serious scholars.

Friedman died on November 2, 1969, and within a year or two the entire collection was shipped to the Marshall Library. Prior to the papers being opened to the public, however, the NSA visited the library and went through the collection. They pulled out two categories of papers and ordered that they be kept locked in a vault and never released. The first category consisted of classified documents which the NSA had agreed to hold for Friedman at Fort Meade. The second, however, despite the wishes of the late cryptologist consisted of totally unclassified, private correspondence between Friedman and other private citizens.

Nevertheless, despite the NSA restrictions, the library allowed me to review and make copies of Friedman's unclassified personal correspondence files. These consisted mostly of letters to and from other private citizens about family matters and personal feelings about the NSA. Nothing in the letters, which were dated mostly from 1955 until 1965, could be considered in any way damaging to the national security and I therefore quoted from them extensively in my book.

Seeing my references to the Friedman letters, the NSA in April of this year went back down to the library and again pulled many of Friedman's unclassified letters and papers from the open shelves, stamped them secret, and locked them in the vault. This despite the Reagan administration's own executive order on secrecy which limits classification to material that is owned by, produced by or for, or is under the control of the United States Government.

Thus, although the letters and documents, unclassified for two to three decades, are quoted in more than 150,000 copies of my book, the NSA insists that they remain "secret." "Just because information has been published doesn't mean it should no longer be classified," said NSA Director Faurer.

In the Reagan administration's war on words there is perhaps no issue more frightening than the issue of reclassification. It would be total anarchy for historians and scholars, who frequently spend years on their research, if one administration would be permitted to recall history by forcing them to return materials released by a previous administration. The NSA offers a perfect example of what happens when an agency is allowed to run wild with the classification stamp. It is a choice of history or hysteria.

About 350 years ago Cardinal de Richelieu declared the principle under which the Reagan Administration currently operates: "Secrecy is the first essential in affairs of the State."

Mr. KASTENMEIER. Thank you, Mr. Bamford.

I am sorry, I did misrepresent that you once had worked for the National Security Agency. In fact, you had not; is that correct?

Mr. BAMFORD. That is true.

Mr. KASTENMEIER. Yes.

Now, Mr. Ralph McGehee, will you proceed, sir?

Mr. McGEHEE. Thank you, Mr. Chairman.

I appreciate the invitation to appear before the subcommittee to discuss my experiences with the CIA's prepublication review requirement.

I am a retired CIA officer who earned numerous awards and medals, including the prestigious Career Intelligence Medal.

During my last 10 years with the CIA, I protested false information on Vietnam. The deficiencies that created Vietnam permeate CIA operations, and I felt an imperative to tell this to the American people and wrote a book about my experiences. The book did not attempt to reveal the identities of my associates or other classified information.

I had opted for early retirement in 1977 and immediately began research for a book. I was confused about how to proceed. I couldn't contact publisher, for anything I might tell him might violate pre-publication review restrictions.

So I decided to work alone without benefit of a contract or guidance from an editor. This was a mistake that cost me 2 years of misguided effort.

In February 1980, following 3 years of research and writing, I submitted a manuscript to the CIA. A month later the Agency's Publications Review Board notified that it had identified 397 classified items. These ranged in length from one word to several pages.

Over the next weeks I worked with a representative of the PRB to prove that those deleted passages did not contain classified information. I sourced my claims primarily to information appearing in the cleared writings of other Agency authors, such as Colby and Cline and Dulles.

We agreed on a number of revisions, and I rewrote the text accordingly. Dismayed that I had defeated its claims of secrecy, the PRB reversed earlier decisions and began classifying information that only a short time before it said was not classified. This forced me to again prove many of those claims false and to rewrite the text.

Finally, I overcame all objections, and for the first time I had a manuscript to shop around to publishers. Sheridan Square Publications agreed to publish the manuscript only if I would rewrite it as an autobiography, and to do this I prepared an outline as an aid. In the transmitting letter I said I wanted the outline for discussions with an editor, following which I would rewrite and resubmit the manuscript to the CIA.

The PRB refused to deal with the manuscript, yet a little while later they found out that I was going to speak before an academic association, and they requested my speech, even if it was only in outline form—serving a double standard there.

After I had submitted three chapters of the rewrite, the PRB demanded that I complete the entire book before it would release any of the material. I then had to go about rewriting the text without the opportunity of consulting with an editor.

Led by William Casey, the CIA in early 1982 decided, regardless of the legalities, to stop my book. It was not going to let me publish the book.

It attempted to do this by reclassifying everything of substance that was in my first chapter. When I pointed out that this violated the Executive order then in existence, the PRB responded, "That is too bad, we are doing it anyhow."

The CIA was determined to prevent publication of my exposé. It ruled that the entire second chapter was classified, and the second chapter dealt primarily with my personal life, my family life.

I contacted the Washington Post and the subsequent public exposure forced the CIA to relent. If the Post had decided not to run the story, my book would have died there.

Embarrassed by the Post article, the PRB assigned a representative to work with me. Finally, in mid-1982, after more than 5 years of struggle, I had a cleared manuscript.

It was only intense anger and bitterness over Vietnam and a certainty that we would repeat that mistake that motivated me to fight the CIA. At various times I felt defeated and just stopped all my efforts.

But ultimately, anger and concern drove me on. Others who don't have this same overwhelming issue certainly will not endure the frustration.

The CIA claims that it does not use prepublication review to conceal violations of law or to prevent embarrassment. For me it did just that.

The CIA further asserts that it follows the paramount principle of evenhanded and fair treatment for all authors. This is demonstrably not true, and I know of authors it has assisted in writing their books.

Since 1977, the CIA has processed more than 62,000 pages of material, but it does not maintain an institutional memory of released information. This is a deliberate attempt to keep its capability low so it will not have to use that capability when dealing with critics.

Magazines have requested me to write articles very recently. One time I wrote an article, and set up a schedule to deliver it to the legal counsel of the CIA. On reflection I thought if I turn this in then the Agency is going to classify this information, and I will lose my right to even discuss it. At that point it was a nebulous issue whether it was classified or not. I assumed it wasn't, but if they ruled it classified, then I couldn't even discuss it.

Other occasions, I have wanted to write Op-ed pieces and letters to the editors, but I have always stopped because I fear now if I go back to the PRB they are going to classify overt information and stop me from even discussing these issues.

I think it is particularly relevant to relate some of the things that happened to me as I tried to live up to all the strictures of the secrecy agreement that I had signed in 1952. My efforts met only with CIA suspicion. I was placed under surveillance. My phone is tapped, and my mail has probably been opened.

Blatant surveillance is conducted not to determine my actions, but to frighten me into silence. Agency security people have walked my heels in supermarkets, sit in cars near my house, and probably entered my hotel room and removed documents. I have been harassed overseas.

On one occasion a phone monitor was getting a little bit upset at what was being said, and he broke in and started interjecting his objections.

Intimidation is the purpose of all this activity, and I am well aware that Big Brother is watching.

From my experience, I conclude that the CIA, reacting as any bureaucracy, uses prepublication review and spurious claims of national security to prevent the American people from learning of its illegal and embarrassing operations. It attempts to deny to the American people information essential to the good of the Nation and to our democratic processes.

The CIA's efforts demonstrate what we can expect from other agencies, given the same authority under President Reagan's Executive order.

The national security state regards truth as its greatest enemy and cries national security to destroy our freedoms. I fervently hope that something can be done to prevent this from happening.

Thank you, Mr. Chairman.

[The complete statement follows:]

PREPARED STATEMENT OF RALPH W. MCGEEHEE, AUTHOR OF DEADLY DECEITS—MY 25 YEARS IN THE CIA

I appreciate the invitation to appear before the subcommittee to discuss my experience with the Central Intelligence Agency's prepublication review requirement. The issue is of paramount importance as President Reagan's March, 1983 Executive order places hundreds of thousands of Government employees under identical constraints. Supreme Court decisions and liberal interpretations of the executive order could extend life-long prepublication review constraints over an additional several million government employees and employees of firms doing classified Government work. This is a major threat to our constitutionally guaranteed right of free speech and forbodes the approach of 1984 and the national security state.

I am a retired CIA officer who earned numerous awards and medals including the prestigious Career Intelligence Medal. During my last 10 years with the CIA I protested its false information on Vietnam. The deficiencies that created the Vietnam war permeate CIA operations and I felt it imperative to tell this to the American people and wrote a book about my experiences. The book did not attempt to reveal the identities of my associates or other classified information. In an ensuing 2-year battle with CIA censors Mark Lynch an attorney with the American Civil Liberties Union provided advice and excellent legal support.

I had opted for early retirement in 1977 and immediately began research for a book. I feared possible CIA retribution if it discovered I was writing an expose and attempted to keep my activities secret from friends and from family members not living at home. My fears were justified as the CIA soon discovered what I was doing and placed me under close, intimidating, multiple types of surveillance. A surveillance that continues to this day.

I was confused about how to proceed. I could not contact a publisher for anything I might tell him might violate prepublication review restrictions. I decided to work alone without benefit of a contract or guidance from an editor. This was a mistake that cost 2 years of misguided effort.

On February 26, 1980 following 3 years of research and writing, I submitted a manuscript to the CIA. A month later the publications Review Board [PRB] notified me that it had identified 397 classified items in the text varying in length from one word to several pages. Over the next weeks I worked with a representative of the PRB to prove that those deleted passages did not contain classified information. I sourced my claims primarily to information appearing in the cleared writings of other agency authors. We agreed on a number of revisions and I rewrote the text accordingly. Dismayed that I had defeated it claims of secrecy the PRB reversed earlier decisions and began classifying information that only a short time before it had judged to be not classified. This forced me to again prove many of those claims false and to rewrite the text. Finally I overcame all objections and for the first time I had a manuscript, truncated as it was, to shop around to publishers.

The search for a publisher was a long time-consuming effort. Many publishers admitted I had a viable manuscript but all said it needed better focus and rewriting. None but a small ideologically-motivated publisher would risk the time and uncertainty of battling the CIA's review process.

Sheridan Square publications agreed to publish the manuscript only if I would rewrite it as an autobiography. As an aid I prepared a 50-page outline and sent it to the PRB. In the transmitting letter I advised that I only wanted the outline for discussions with an editor following which I would rewrite and resubmit the manuscript. The PRB refused to deal with an outline. (Yet a few weeks later the CIA learned that I was to give a speech to the Association of Asian studies and sent me a registered letter advising that I must submit the speech for review even if only in outline form.) After I had submitted three chapters the PRB demanded that I complete the entire rewrite before it would release any material. I then had to rewrite the remaining text without the opportunity of consulting my editor.

Led by William Casey the CIA in early 1982 decided regardless of the legalities to stop my book. It attempted to do this by reclassifying everything of substance that was in my first chapter. When I pointed out that Executive Order 12065, then in effect, section 1-607 said "classification may not be restored to a document already

declassified and released to the public under this order and prior orders." the PRB responded in essence that that was tough.

The PRB had ruled that I could not discuss my training or the training site at Camp Peary even though such topics had been declassified and well publicized. More oddly the PRB ruled that details of the personality test it gives recruits were classified. Yet a proprietary company had copyrighted and published the test. Also, Jack Anderson's column had carried, in over 1,000 newspapers, those same details that the CIA was claiming were classified.

I appealed those and other decisions to Admiral Inman then the Deputy Director of the CIA. He recognized the total illegality of the Board's decisions and ruled in my favor in every single instance.

The CIA, however, was determined to prevent publication of my expose. It ruled that the entire second chapter was classified. I contacted the Washington Post and the subsequent public exposure forced the CIA to relent. If the story had not run it would have been the end of my book. Embarrassed by the Post's article the PRB assigned a representative again to work with me over the classified items and I again rewrote and resubmitted the manuscript. Finally in mid-1982, after more than 5 years of struggle, I had a cleared manuscript.

It was only intense anger and bitterness over Vietnam and the certainty that we would repeat that mistake that motivated me to fight the CIA. At various times I felt defeated and ceased my efforts. But ultimately anger and concern drove me on. Others not motivated by such an overwhelming issue will not endure the frustration.

The CIA avers that it does not use prepublication review to conceal violations of law or to prevent embarrassment. For me it did just that and claimed secrecy to conceal its illegal and inefficient operations. The CIA further asserts that it follows the paramount principle of evenhanded and fair treatment for all authors. This is demonstrably not true. It assists the writings of proponents while suppressing the works of critics. Since 1977 the CIA has processed more than 62,000 pages of material but maintains no institutional memory of released information. This is not bureaucratic inefficiency, it is the deliberate crippling of its own ability. If the CIA kept records of cleared information it might be forced to use that memory when dealing with critics. This it avoids at all costs.

Magazines have recently requested me to write articles for them. I went about conducting the research and preparing drafts. But upon reflection I worried that if I submitted the articles to the CIA for review it would again classify overt information and I would lose my right to even discuss those issues. I decided not to take the risk and informed the magazines that I could not write the articles for them.

On various other occasions I had wanted to write letters to the editor or op-ed pieces for newspapers. Each time I stopped because I feared the consequences. Due to prepublication review and the inevitable use of that authority by the CIA to suppress criticism, my informed opinion on a range of topics is not available for public debate. Multiplying the constraints on me by the hundreds of thousands or possibly millions of Government employees subject to the new executive order, the result is obvious and calamitous. Informed criticism of the processes of Government will be repressed and those essential contributions to the maintenance of our democratic institutions will be stilled.

It is of particular relevance to the topic of this hearing to relate some of my experiences as the CIA monitored by activities. I have lived up to all the requirements of the secrecy agreement I signed in 1952. My efforts have met only with CIA suspicion. I have been placed under surveillance, my phone is tapped and my mail has probably been opened. Blatant surveillance is conducted not to determine my actions but to frighten me into silence. Agency security personnel have walked up my heels in supermarkets, sit in cars near my house and have probably entered my hotel room and removed documents. I have been harassed overseas in Canada. On one occasion a phone monitor interrupted a conversation to protest what was being said. Intimidation is the purpose of all this activity and I am well aware that "Big Brother Is Watching."

From my experiences I conclude that the CIA, reacting as any bureaucracy, uses republication review and spurious claims of national security to prevent the American people from learning of its illegal and embarrassing operations. It attempts to deny to the American people information essential to the good of the Nation and to our democratic processes. The CIA's efforts demonstrate what we can expect from other agencies given the same authority under President Reagan's executive order.

The national security state regards truth as its greatest enemy and cries national security to destroy our freedoms. I fervently hope that something can be done to prevent this from happening. Thank you.

Mr. KASTENMEIER. Thank you, Mr. McGehee. Do you attribute what you term harassment and surveillance, to the fact that you are engaged in seeking to publish material concerning the CIA or, because of the bitterness you feel about the Vietnam war, your views are at odds with Agency policy?

Mr. McGEHEE. I am sure if I were a proponent of the Agency that I would not be subject to any of this activity. The fact that I am a critic I think is the reason they surveil me.

Mr. KASTENMEIER. It would appear from the statement you have filed with us that you have submitted your testimony to the Central Intelligence Agency for prepublication review.

Mr. McGEHEE. That is correct.

Mr. KASTENMEIER. And they cleared it?

Mr. McGEHEE. Yes; they did.

Mr. KASTENMEIER. Does that surprise you, considering—

Mr. McGEHEE. Oh, no. If this were an article that I was writing, there would have been a great deal of argument back and forth, but since I was submitting this to a congressional committee, I assumed that they would be very lenient and let me say anything that I wanted to say.

Mr. KASTENMEIER. If they had chosen to do otherwise, would you have complied with their request?

Mr. McGEHEE. I always have; yes, sir.

Mr. KASTENMEIER. You always have?

Mr. McGEHEE. Yes.

Mr. KASTENMEIER. Mr. Bamford, the essence of your complaint is because of a new policy called reclassification. Is that truly a new policy?

Mr. BAMFORD. Yes; it is. It is new under the Reagan administration. Under the Carter administration, the way the Executive order on secrecy read was that once a document had been declassified it could not be reclassified again. Once the information had been released to the public, you can't recall it.

That policy has been completely reversed under the Reagan administration. So, in other words, if somebody was working on a history of the Johnson administration, somebody in the Reagan administration can go back and say that although you obtained that information under the Johnson administration it is now classified and you cannot use that anymore.

Mr. KASTENMEIER. You have also asserted that there is an attempt to regain material from you which has now been reclassified, is that correct?

Mr. BAMFORD. Yes.

Mr. KASTENMEIER. Is that a separate complaint; that is, is it divorced from the other?

Mr. BAMFORD. Well, all these come under the heading of reclassification.

The first attempt was by the Reagan administration to recall 250 pages worth of Justice Department documents that were released to me under the Carter administration. They threatened to use the espionage statute if I didn't give the materials back.

But at the time they made those requests, the Reagan administration was still operating under the old Carter administration Ex-

Executive order, and that was one of the reasons why President Reagan changed the Executive order to the way it stands now.

After my book came out, Reagan administration, actually the NSA [National Security Agency] went down to one of the libraries I used and began pulling off the shelves papers and documents that I had quoted from and stamped those documents secret and ordered that they be locked in a vault.

Mr. KASTENMEIER. As I recall, you litigated this problem; is that correct?

Mr. BAMFORD. No. I had an attorney, Mark Lynch, from the American Civil Liberties Union, but we settled out of court basically on the issue of the original documents, and on the second issue I never litigated because the material was already in my book. So I didn't feel any need to litigate the issue.

Mr. KASTENMEIER. To your knowledge, or in your estimation, are there many other individuals—researchers and writers and others—who are going to have similar difficulty with reclassification, or is this a unique experience?

Mr. BAMFORD. Well, Mr. Chairman, it is fairly unique. There are one or two other instances I have heard of.

One instance was a writer who was working on a book dealing with the U.S. relationship with Israel, and the individual requested some documents from the National Archives, and the documents were sent to him. They were declassified and sent to him.

Later on, the Archives asked to have those documents sent back to the Archives for some review. Once they were sent back, however, they were reclassified in accordance with an order from the Air Force, and there was a lawsuit over that issue, and the Air Force and the Archives more or less retreated and released the documents once again.

I understand there was one other incidence involving some material from the Drug Enforcement Administration.

It is an issue which will probably come up time and time again if the administration is allowed to proceed with these cases without any inquiry or without any objection.

Mr. KASTENMEIER. Mr. McGehee, in your case you did litigate your problem with the Agency to the D.C. Court of Appeals in the Federal Circuit?

Mr. McGEHEE. Yes, sir.

Mr. KASTENMEIER. You lost your suit, is that correct?

Mr. McGEHEE. I did sue over deletions that were made in an article that I had written for the Nation magazine, and this has been under litigation for 2½ years, and the U.S. district court of appeals just recently ruled that the Agency was justified in making the deletions.

I don't think all the issues were brought forward, and my lawyer is going to file an appeal for a rehearing.

Mr. KASTENMEIER. So that matter hasn't been finally judicially concluded?

Mr. McGEHEE. It has not been finally; no.

Mr. KASTENMEIER. I see. Thank you.

I yield to the gentleman from Ohio.

Mr. DEWINE. No questions, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from Michigan.

[No response.]

Mr. KASTENMEIER. We appreciate your appearance, Mr. McGehee and Mr. Bamford, this morning, detailing two experiences with the national security agencies of the Federal Government.

It is helpful to know how policy is changing and what impact it has had on two people in a situation such as this.

I think the matter of reclassification probably has not gotten very much visibility or attention. It is something we ought to look at.

In any event, we are grateful for your appearance, and this concludes the hearing today.

I will announce that, as scheduled, we will be having a hearing tomorrow morning, room 2226 of this building, at 10 a.m., and we will continue our hearings on the subject we initiated today.

Until that time, the committee stands adjourned.

[Whereupon, at 11:40 a.m., the subcommittee was adjourned, to reconvene at 10 a.m., Thursday, November 3, 1983.]

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

THURSDAY, NOVEMBER 3, 1983

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:30 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier and Berman.

Staff present: David W. Beier and Deborah Leavy, counsels; Joseph V. Wolfe, associate counsel; and Audrey Marcus, clerk.

Mr. KASTENMEIER. The committee will come to order.

Today we continue a set of hearings begun yesterday on 1984, civil liberties and the national security state. The focus of today's hearing is the conflict between academic freedom, scientific communication, and restrictions thereon based on national security considerations.

Our first witness will be C. Peter Magrath, and I note that one of our colleagues and close friend of the president of the University of Minnesota is here. Perhaps he would like to present Dr. Magrath to the committee. I am talking about Congressman Jim Oberstar.

Mr. OBERSTAR. Thank you very much, Mr. Chairman.

I will spare you, the committee and myself, a long introduction. With this virus I have, my voice is not in form. But it is an honor and a privilege to present Dr. Peter Magrath, president of the University of Minnesota, who in his tenure has brought a new excitement to the university, an atmosphere of academic ferment and inquisitiveness that is the hallmark of a first-rate academic institution. He has involved himself with the academic affairs of the university in a way that few of his predecessors have done. He has brought a new excitement about the institution and attracted top-level professorial talent to the University of Minnesota. He brings personal warmth and keen insight to all he undertakes, and it is a pleasure for me to present him to the committee.

Mr. KASTENMEIER. We thank our colleague for that generous introduction of Dr. Magrath, which I am sure is well deserved, whom we hope will provide an overview of the potential conflicts between academic freedom and national security, and on the free flow of information.

Also we would ask to join Dr. Magrath another very important witness, Dr. Frank Press, who is president of the National Academy of Sciences and a former Presidential Science Adviser. Dr. Press will address a recent report on national security concerns as they affect the sciences.

We will have following them another panel involving representatives of several other institutions who will address instances of restrictions on scientific information.

So our witnesses will describe in greater detail how the academic and scientific community has increasingly found itself in an adversarial situation with the executive branch. The number of conflicts has led to the appointment of various study committees and commissions. The common theme of the reports issued by these groups is a need to articulate the values that are preserved by the free flow of information. In part, one of the purposes of this morning's hearing is to provide a wider public forum for an expression of these values.

This morning we will address other important policy questions: One, to what extent does the first amendment protect the free flow of scientific information; two, are the values from an unencumbered exchange of information intended to work for the benefit of all Americans, not just academics and scientists; three, is it fair or appropriate to expect the academic and scientific communities to negotiate their first amendment rights with the executive branch; four, what role should the Congress play in calculating the criteria to be used before restrictions are placed on this flow of information. So it is my hope through this hearing and through subsequent submissions from interested parties and organizations that the committee will receive guidance and suggestions about the desirability and the feasibility of legislation in this area.

Before calling on our first witness, I would like to recall the words of James Madison, who said:

Since the general civilization of mankind, I believe there are more instances of the abridgement of the freedom of people by gradual and silent encroachments of those in power than by violent and sudden usurpations.

[The following was received for the record:]

C. Peter Magrath
Testimony Before the House Subcommittee on Courts,
Civil Liberties, and the Administration of Justice
November 3, 1983

Mr. Chairman and Honorable Members of this Committee:

My name is C. Peter Magrath, and I am President of the University of Minnesota. I appreciate the invitation to discuss with you a concern shared by a growing number of university presidents and their faculties.

Broadly stated, the concern involves a conflict between openness and secrecy, between academic freedom and prior restraint, between the pursuit of knowledge and the definition of national security. More specifically, the conflict grows out of the Administration's efforts to advance American defense interests by restricting the free flow of information among scientists, researchers, and engineers.

The restrictions, which have been issued by the Departments of Defense, State, Commerce, and Energy over the past 2½ years, take a variety of forms.

— There are Presidential directives that authorize prior governmental review of any publication by individuals who ever had access to classified information, and presumably, this includes university scholars as well.

— There are regulations that permit the Executive Branch to restrain the presentation, publication, or mere scholarly exchange of papers that are neither classified nor drawn from classified sources.

— There are instructions to limit the access of certain foreign students and scholars to college classrooms and laboratories.

— And there are surveillance requests to gumshoe international visitors across the campus and the local community.

Specific examples of the first two types of restrictions will be provided by other speakers, but permit me to offer a personal experience which illustrates the latter two directives.

In 1981, the University of Minnesota received a number of letters, phone calls, and campus visits by federal agents regarding a visiting scholar from the People's Republic of China by the name of Qi Yulu. The State Department had previously approved Mr. Qi's study plans under a national policy that expressly "encourages the training of Chinese scholars in modern technology and science." Subsequently, the policy seemed to change, for the University was asked to curtail the academic program of our visitor.

According to the State Department, Mr. Qi was to have no access to unpublished or classified government-funded research; no access to computer hardware design or maintenance; and no access to source codes or their development. In addition, the University was to limit the scholar's access to published software alone; provide him minimal involvement in applied research; and report, in advance, any visits he might make to industrial or research facilities. Ironically, within those constraints, we were told to offer Mr. Qi as full an academic program as possible.

The directives were confusing to say the least. For example, the State Department proposed limiting the scholar's access to classified research, yet in common with virtually all of higher education, the University of Minnesota accepts and conducts no such research. There was to be only minimal involvement in applied research, but a definition of either "minimal" or "applied" was never given. There was to be a full academic program, yet for this computer

scientist, most of our computer technology was off limits. And, of course, there was the problem of advising federal officials as to the constant whereabouts of Mr. Qi Yulu, an assignment that would force the University to confine him or else contact the State Department several times a day as to his on and off campus itinerary.

However, even more disturbing than the confusing nature of the State Department's directives were their chilling implications. They struck at the very heart of a free university, if not a free society, for they advocated secrecy and surveillance, the restraint of expression and the disregard of academic freedom. Scholarship simply cannot thrive in secrecy; research cannot be advanced under wraps. Instead, scientific progress flourishes best in the free competition of ideas. It is that openness and competition which explains why the United States is preeminent in most scientific fields. And it is the absence of openness and competition in the Soviet system which confirms an observation of Nobel laureate, P.W. Anderson, namely, "Security and secrecy impede scientific and technical progress . . . tend(ing) to cloak inefficiency, ignorance, and corruption more often than it hides genuine technical secrets."

This is not to imply that the protection of "genuine technical secrets" is an inappropriate concern of our government. The concern is understandable; the objectives legitimate. Few Americans, and even fewer members of the research community, advocate the dissemination of information that directly compromises national defense. However, what is questionable and alarming are the means by which such objectives are pursued. To attempt to plug national security leaks by muffling those who pose no security risk makes little sense. It amounts to caulking the wrong part of the wrong ship, and in the end, the efforts prove to be unnecessary, intimidating, and counterproductive.

At least four issues merit your consideration here. First, most scientific investigations that are carried out in campus laboratories offer no immediate applications. Consequently, the sharing of such research, even with foreign scholars, poses virtually no threat to U.S. technological or military interests. A National Academy of Science panel on "Scientific Communication and National Security" reached just such a conclusion when it reported that "(U)niversities and open scientific communication have been the source of very little of (America's) technology transfer problem." The view was reinforced in testimony delivered last year by former CIA Director, Bobby Inman. Admiral Inman concluded that "only a small percentage" of the Soviet acquisition of militarily relevant information comes from communications involving scientists and students.

Second, to force scholars to clear studies prior to publication presents an impossible burden for researcher and reviewer alike. That task is to define the importance of undefined knowledge, to predict the outcome of incomplete investigations, and to articulate the possible consequences of unknown applications. On the part of a scientist, it is akin to requiring Albert Einstein in his early spectroscopy research to foresee the creation of laser technology some half century later. On the part of government review teams, it is to encourage restrictive decisions, because without a clear understanding of possible applications, there is an inevitable tendency to err on the side of caution and censorship.

A third problem is that of interpreting vague and sweeping regulations. The task is not only confusing, but it is also intimidating. There is a price to be paid for compliance as well as non-compliance. For example, current State Department regulations can require a university to supply background information on students, yet in releasing such information, the school runs

the risk of violating the Federal Educational Rights and Privacy Act as well as State privacy statutes. Similarly, cooperation could force a university to adopt a policy requiring its faculty to submit certain publications to government review, yet in so doing, the institution runs the risk of being a willing party to prior restraint and First Amendment violations.

On the other hand, the price of non-compliance is no less threatening. A university that misinterprets the complex International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations (EAR) exposes itself to administrative and civil penalties and fines not to mention the forfeiture of federal contracts. The loss to the uncooperative institution is further compounded by the possibility of being "blacklisted." I know of five university presidents who received just such a warning from a private foundation. The foundation promised to sponsor adverse shareholder resolutions at corporate and philanthropic meetings, because it determined that resistance to intrusive regulations was itself a threat to national security.

A fourth issue -- the imposition of restraints upon scholarly exchanges -- is equally disturbing. One justification, at least according to the Director of the Office of Military Technology in the Defense Department, is "to restrict Soviet scientists in the way American scientists are restricted in the Soviet Union." At best, the rationale is ironic; at worst, it is counterproductive.

It is ironic that the secrecy of a governmental system we disdain should become a model for our own research policies -- a standard, by the way, that has been applied not only to Soviet scholars, but to visitors from the People's Republic of China, the Middle East, and Eastern Europe.

It is counterproductive in that much of our knowledge about Soviet advances in metallurgy, astrophysics, robotics, cancer research and other fields is a direct result of communication between U.S. and Russian scholars. To restrict those exchanges is both to forfeit an invaluable information conduit and to overlook those areas where American science has been furthered through exposure to Soviet contacts.

In short, Mr. Chairman, the issues and problems I have raised require a greater sensitivity on the part of this Administration. To that end, there have been a number of recent discussions among university and cabinet representatives. However, because change is so slow in coming, Congressional action might well have to be taken if the concerns of the research community are to be taken seriously. In prompting such change, let me conclude with the following recommendations:

First, the majority of the restraints upon scholars and scientists appear to be unilaterally imposed by the Executive Branch, rather than flowing from express grants of legislative authority. In the absence of any modification in those restraints, Congress must give serious consideration to imposing clear structural limits upon administrative interpretations.

Second, only in the most exceptional and limited cases should the communication of unclassified scientific information be restricted. Any other course would not only transform much unclassified information into classified information, but even more significantly, it would impede the very avenues for scholarly communication that are so vital to national security.

Third, if certain research is to be classified, then a mandatory review mechanism should be implemented. One framework for such review has been proposed by the Department of Defense Forum, an advisory body that was established twenty months ago and that includes representatives from the DOD and the university community. Even as I applaud certain DOD officials for taking the initiative in establishing this communication channel, I would encourage other Cabinet departments to follow the Defense Department's lead. By institutionalizing dialogue, some of the differences between the Capitol and the campus can be resolved in advance of regulatory overkill and public disputes.

Fourth, the university community recognizes that under exceptional and narrowly defined circumstances, restrictions on foreign scholars may be appropriate. These restrictions should not, by definition, be targeted at our open universities, but would apply to such non-university activities and locations as classified laboratories operated by defense contractors. Clearly, in the vast majority of cases, restraints on scholarly exchanges must be avoided if this nation is committed to improving relations with foreign countries, to reducing bureaucratic expenses, and to enhancing our own scientific capacities.

Fifth, if there are reservations as to the activities of certain visiting scholars, then it is the responsibility of the State Department to resolve those reservations before the scholars are granted permission to enter the country. It is not the function of the academy to be a surrogate surveillance agency.

Sixth, if there are to be restrictions on certain types of scientific activities -- in other words, secret research -- then such activities should

be classified in advance, thereby putting universities on notice of the restrictions before they apply for the contract. Alternatively, serious consideration should be given to a policy of conducting all secret research in government laboratories or private institutions rather than universities. If the price of government research contracts is the forfeiture of open scholarly communication, then the tradeoff is simply too high.

Seventh, there should be an immediate clarification of the executive orders requiring individuals with access to what is now labelled "sensitive compartmented information" to sign pre-publication clearance agreements and to submit to lie detector tests under certain circumstances. To the extent that these orders are intended to apply to universities and faculty members in their roles as federal contractors, such orders should be rescinded. Scholars who contribute a period of their careers to government service or who carry out federal research should not be forced to take lifelong vows of silence. The laboratory is not the monastery; the scientist is not a Trappist monk. To misunderstand these differences is to discourage the best and the brightest from lending their talents to national objectives, and, in that case, our security will truly be jeopardized.

In short, Mr. Chairman, if the question is whether our national interests are better served by openness and technological progress or by secrecy and scholarly restraints, then I would urge you to choose the former. The history of this nation is one of security by scientific accomplishment. It has enabled us to outpace our adversaries in the past, and it will permit us to continue our lead in the future. America simply does not need the Soviet model of science or the Soviet system of secrecy and surveillance!

Mr. KASTENMEIER. I would now like to call on the president of the University of Minnesota, Dr. Magrath.

TESTIMONY OF C. PETER MAGRATH, PRESIDENT, UNIVERSITY OF MINNESOTA; AND FRANK PRESS, PRESIDENT, NATIONAL ACADEMY OF SCIENCES

Dr. MAGRATH. Thank you very much, Mr. Chairman.

As indicated, my name is C. Peter Magrath and I am privileged to serve as president of the University of Minnesota. I am also privileged to work in a State that has elected so many outstanding Members of Congress and the Senate, one of whom took time from his very hectic schedule, Congressman Oberstar, to come here this morning.

To Congressman Oberstar, I want to say that those of us in the university community, not only in the University of Minnesota, appreciate a person who understands what research universities are about and what the role of great private and public universities is about. We don't take that kind of understanding and support lightly, and I personally appreciate his support enormously.

I appreciate this opportunity to discuss with you the concern, Congressman Kastenmeier, that you have stated, because it is one that is shared by a large number of university presidents and their faculties. In broad terms, the concern is a conflict between openness and secrecy, between academic freedom and prior restraint, between the pursuit of knowledge and the definition of national security. More specifically, the conflict arises out of the administration's efforts to advance American defense interests—which are legitimate, of course, very legitimate—by restricting in various ways the free flow of information among scientists, researchers, and engineers.

The restrictions which have been issued by the Departments of Defense, State, Commerce, and Energy over the past 2½ years take a variety of forms:

There are Presidential directives that authorize prior governmental review of any publication by individuals who ever had access to classified information, and presumably, this seems to include university scholars as well.

There are regulations that permit the executive branch to restrain the presentation, publication, or mere scholarly exchange of papers that are neither classified nor drawn from classified sources.

There have been instructions to limit the access of certain foreign students and scholars to college classrooms and laboratories.

And there have been surveillance requests to, in effect, gumshoe international visitors across the campus and the local community.

Specific examples of the first two types of restrictions will be provided I believe by other witnesses, but permit me to offer first a personal experience that illustrates the latter two directives.

In 1981, the University of Minnesota received a number of letters, phone calls and campus visits by Federal agents regarding a visiting scholar from the People's Republic of China by the name of Qi Yulu. The State Department had previously approved Mr. Qi's study plans under a national policy that expressly—and I quote—

"encourages the training of Chinese scholars in modern technology and science." Subsequently, the policy seemed to change, for the University of Minnesota was asked to curtail the academic program of our visitor.

According to the State Department, Mr. Qi was to have no access to unpublished or classified Government-funded research, no access to computer hardware design or maintenance, and no access to source codes or their development. In addition, we were to limit his access to published software alone, provide him minimal involvement in applied research, and report, in advance, any visits he might make to industrial or research facilities. Ironically, within these constraints, we were told to offer Mr. Qi Yulu as full an academic program as possible.

The directives were confusing to say the least. For example, the State Department proposed limiting the scholar's access to classified research, yet in common with virtually all of higher education, the University of Minnesota accepts and conducts no such research. There was to be only minimal involvement in applied research, but a definition of either "minimal" or "applied" was never given. There was to be a full academic program, yet for this computer scientist most of our computer technology was to be off limits. And, of course, there was the problem of advising Federal officials as to the constant whereabouts of Mr. Qi Yulu, an assignment that would force us to confine him or else contact the Department of State several times a day as to his on and off campus itinerary.

Much more disturbing perhaps than the confusing nature of these directives were their chilling implications. They struck I believe at the very heart of a free university, if not a free society, for they advocated secrecy and surveillance, the restraint of expression, and the disregard of academic freedom. Scholarship simply cannot thrive in secrecy; research cannot be advanced under wraps. Instead, scientific progress flourishes best in the free competition of ideas. It is that openness and competition which explains why the United States is preeminent in most scientific fields. It is the absence, I submit, of openness and competition in the Soviet system that confirms an observation made by the Nobel Laureate P.W. Anderson, namely, "Security and secrecy impede scientific and technical progress * * * tending to cloak inefficiency, ignorance, and corruption more often than it hides genuine technical secrets."

This is not to imply that the protection of "genuine technical secrets" is an inappropriate concern of our Government. That concern is understandable, and the objectives legitimate. Few Americans, and even fewer members of the research community, advocate the dissemination of information that directly compromises national defense. However, what is questionable and alarming are the means by which these legitimate objectives are pursued.

To attempt to plug national security leaks by muffling those who pose no security risks at all makes little sense. It amounts, if you will, to caulking the wrong part of the ship, and of the wrong ship at that, and in the end the efforts prove to be unnecessary, intimidating, and counterproductive.

I think there are at least four issues that merit your consideration. First, most scientific investigations that are carried on in campus laboratories offer no immediate applications. Consequently, the sharing of such research, even with foreign scholars, poses virtually no threat to U.S. technological or military interests. A National Academy of Science panel, chaired by the very distinguished former president of Cornell University, on "Scientific Communication and National Security" reached precisely this conclusion when it reported that "Universities and open scientific communication have been the source of very little of America's technology transfer problem." That view was reinforced in testimony delivered last year by former CIA Deputy Director Bobby Inman. Admiral Inman concluded that "only a small percentage" of the Soviet acquisition of militarily relevant information comes from communications involving scientists and students.

Second, to force scholars to clear studies prior to publication presents I think an impossible burden for researcher and reviewer alike. That task is to define the importance of undefined knowledge, to predict the outcome of incomplete investigations, and to articulate the possible consequences of unknown applications. On the part of a scientist, it is akin to requiring Albert Einstein in his early spectroscopy research to foresee the creation of laser technology some half-century later. On the part of Government review teams, it is to encourage restrictive decisions, because without a clear understanding of possible applications, there is an absolutely inevitable tendency to err on the side of caution and censorship.

A third problem is that of interpreting vague and sweeping regulations. The task is not only confusing, but it is intimidating. There is a price to be paid for compliance as well as noncompliance. For example, current State Department regulations can require a university to supply background information on students; yet, in releasing such information, the school runs the risk of violating the Federal Educational Rights and Privacy Act as well as State privacy statutes. Similarly, cooperation could force a university to adopt a policy requiring its faculty to submit certain publications to Government review, yet in so doing the institution runs the risk of being a willing party to prior restraint and first amendment violations.

On the other hand, the price of noncompliance is no less threatening. A university that misinterprets the complex International Traffic in Arms Regulations [ITAR], or the Export Administration Regulations [EAR], exposes itself to administrative and civil penalties and fines, not to mention the forfeiture of Federal contracts. The loss to the uncooperative institution is further compounded by the possibility of being "blacklisted". I know of five university presidents who received just such a warning from a private, not a governmental, but from a private foundation. The foundation promised to sponsor adverse shareholder resolutions at corporate and philanthropic meetings because it determined that resistance to intrusive regulations was itself a threat to national security. The University of Minnesota was one of those five universities.

A fourth issue, the imposition of restraints upon scholarly exchanges, is equally disturbing. One justification, at least according to the Director of the Office of Military Technology in the Defense

Department, is "to restrict Soviet scientists in the way American scientists are restricted in the Soviet Union." At best, the rationale is ironic; at worst, it's counterproductive.

It is ironic that the secrecy of a governmental system we disdain should become a model for our own research policies—a standard, by the way, that has been applied not only to Soviet scholars but to visitors from the People's Republic of China, the Middle East, and Eastern Europe.

It is counterproductive in that much of our own knowledge about Soviet advances in metallurgy, astrophysics, robotics, cancer research and other fields is a direct result of communications between U.S. and Soviet scholars. Also there is the assumption that we are the ones that are giving something away and that we aren't smart and we don't learn and pick up things. The contrary is true, I believe. To restrict those exchanges is to forfeit an invaluable information conduit and to overlook those areas where American science has been furthered through exposure, in this case to Soviet contacts.

In short, Mr. Chairman, the issues and problems I have raised require a greater sensitivity on the part of this administration. To that end, there have been a number of recent discussions among university and cabinet representatives. However, because change is so slow in coming, congressional action might well have to be taken if the concerns of the research community are to be taken seriously. In prompting such change, let me conclude with the following suggestions:

First, the majority of the restraints upon scholars and scientists appear to be unilaterally imposed by the executive branch, rather than flowing from express grants of legislative authority. In the absence of any modification in those restraints, Congress must give serious consideration to imposing clear structural limits upon administrative interpretations.

Second, only in the most exceptional and limited cases should be communication of unclassified scientific information be restricted. Any other course would not only transform much unclassified information into classified information, but even more significantly, it would impede the very avenues for scholarly communication that are so vital to our national security.

Third, if certain research is to be classified, then a mandatory review mechanism should be implemented. One framework for such review has been proposed by the Department of Defense University Forum, an advisory body that was established 20 months ago and includes representatives from DOD and the university community. Even as I strongly applaud certain DOD officials for taking the initiative in establishing this communication channel, I would encourage other Cabinet departments to follow the Defense Department's lead. By institutionalizing dialog, some of the differences between the Capitol and the campus can be resolved in advance of regulatory overkill and public disputes.

Fourth, the university community recognizes that under exceptional and narrowly defined circumstances restrictions on foreign scholars may be appropriate. These restrictions should not, by definition, be targeted at our open universities, but would apply to such nonuniversity activities and locations as classified laboratories

operated by defense contractors. Clearly, in the vast majority of cases, restraints on scholarly exchanges must be avoided if this Nation is committed to improving relations with foreign countries, to reducing bureaucratic expenses, and to enhancing our own scientific capacities.

Fifth, if there are reservations as to the activities of certain individuals who are to come to the United States under the cloak of being a visiting scholar, then it is the responsibility, I suggest, of the Department of State to resolve those reservations before the scholars are granted permission to enter the country. It is not the function of the academy to be a surrogate surveillance agency.

Sixth, if there are to be restrictions on certain types of scientific activities—in other words, secret research—then such activities should be classified in advance, thereby putting universities on notice of the restrictions before they apply for the contract. Alternatively, serious consideration should be given to a policy of conducting all secret research in Government laboratories or private institutions rather than universities. If the price of Government research contracts is the forfeiture of open scholarly communication, then the tradeoff is simply too high.

Seventh, there should be an immediate clarification of the Executive orders requiring individuals with access to what is called "sensitive compartmented information" to sign prepublication clearance agreements and to submit to lie detector tests under certain circumstances. To the extent that these orders are intended to apply to universities and faculty members in their roles as Federal contractors, such orders should be rescinded. Scholars who contribute a period of their careers to Government service or who carry out Federal research should not be forced to take lifelong vows of silence. The laboratory is not the monastery; the scientist is not a Trappist monk. To misunderstand these differences is to discourage the best and the brightest from lending their talents to national objectives and, in that case, our security will truly be jeopardized.

In short, Mr. Chairman, if the question is whether our national interests are better served by openness and technological progress, or by secrecy and scholarly restraints, then I would urge you to choose the former. The history of this nation is one of security by scientific accomplishment. It has enabled us to outpace our adversaries in the past, and it will permit us to continue our lead in the future. America simply does not need the Soviet model of science or the Soviet system of secrecy and surveillance.

Thank you for hearing my remarks.

Mr. KASTENMEIER. Thank you, Dr. Magrath. I want to compliment you for a splendid and clear statement. Before we go to questions, however, we will hear from Dr. Frank Press.

Dr. PRESS. Thank you, Mr. Chairman.

Many of my comments today will be based on a report of the Academy, the Corson Report on "Scientific Communication and National Security", which President Magrath referred to.

The subject of this hearing has become a national issue basically because advancing scientific knowledge—and, more importantly, the technology that is founded on that knowledge—has brought two legitimate social objectives into conflict: the advancement of knowledge and the Nation's military security.

With the exception of wartime, free international scientific communication rarely has been perceived as detrimental to America's defenses against foreign military adversaries. However, initiatives have been undertaken over the past several years to prevent the dissemination of certain U.S. research results from providing military advantages to America's adversaries. The reaction to these measures has included strong statements of principle both by advocates of scientific freedom and of national security; that is, statements vigorously decrying and supporting such measures.

The issue, in my view, is somewhat paradoxical, for the quality of our new military and commercial technologies derives from U.S. scientific superiority, and that superiority depends upon the open exchange of ideas. The health of the research enterprise depends crucially on scientists building on each others' ideas and on the ability to test new ideas against the best existing ideas worldwide. The informal exchange of draft scientific papers among leading specialists in the field, travel to scientific meetings and conferences, personnel exchanges, and the publication of papers and their exposure to global scrutiny by other researchers is the essence of productive science. It is, I think, no accident that a nation founded on personal liberties enjoys world leadership in science, and it is no accident that closed societies have been forced to look outward for the science that must underlie their technological advances.

Thus, American scientists are extremely sensitive to the possibly chilling effects of various governmental efforts to control scientific communication. These include attempts to prevent certain unclassified research results from being presented at meetings attended by scientists from Warsaw Pact countries. This occurred, for example, at a meeting on magnetic bubble devices held by the American Vacuum Society in 1980, at the annual technical symposium of the Society of Photo-Optical Engineers in 1982, and at the Fourth International Conference of Permafrost in 1983.

There are also initiatives to require scientists to secure governmental permission before they make their unclassified research results accessible in foreign countries. That would, of course, include virtually all scientific publications, since almost all have an international readership. An example is the "no foreign distribution" condition in some unclassified governmental research contracts.

Perhaps most disquieting, from the point of view of individual United States scientists, is that these and other governmental actions to control scientific communication have been largely disjointed, unpredictable, and vague in specifying the scientific fields they are intended to cover. The result is that any particular scientist is quite unclear about what obligations and sanctions, if any, might apply to her or his work.

More generally, advocates of openness in science point out that imposing national security controls on scientific work may be counterproductive. For example, restrictions on scientific meetings held in the United States may result in international scientific organizations banning meetings in the United States and the relocation of these meetings to other sites that are more accessible to foreign scientists and less accessible to ours.

Also, as the international scientific enterprise continues to advance, the proportion of scientific fields in which United States sci-

ence has a clear lead will diminish, meaning that international communication in more and more fields will be in our own scientific and technological interest.

Finally, there is same danger that in those scientific areas where controls are imposed, some of the best United States scientists and, importantly, some of their best students, will simply transfer their interest to unrestricted research areas, thus depriving military and civilian technologies of their contributions.

Proponents of stricter controls offer arguments that must be seriously evaluated. They point out that increasingly United States security is related to our technological lead over our military adversaries. The days in which the advantage went to the Nation with the largest military, the best trained soldiers, or the most defensible boundaries are largely behind us. Second, they point out that military technology is increasingly what is called high technology; that is, more and more critical military technologies are in areas that are very close to current scientific frontiers. In addition, many of these new technologies are dual use technologies, like advanced electronics, having both military and civilian applications. The significance of the rise of dual-use technology is that one can no longer be certain, even if research is not funded by the military, that it will be irrelevant to military needs.

Citing these trends, those whose job is to protect United States national security often point to the danger that we thoughtlessly give away the advantage of our scientific superiority in critical fields.

Both points of view are based on legitimate concerns. The objectives of the Academy study by the Corson Panel were to consider those concerns, to examine the evidence, and to explore ways to resolve the dilemma. The organization and mission of the Panel on Scientific Communication and National Security was designed to ensure that it received views from all sides of the issues. Its membership included several former national security officials, as well as university and industry scientists. Furthermore, the Panel solicited evidence and differing views from many groups.

The Panel offered 15 specific recommendations, and these recommendations rested on four basic findings:

First, although there is substantial evidence of damaging transfers of military technologies to the Soviet Union, and of Soviet interest in acquiring Western science by both overt and covert means, the Panel found that—and I quote—“in comparison with other channels of technology transfer, open scientific communication involving the research community does not present a material danger from near-term military implications.”

The Panel carefully evaluated both published and highly classified information of known technology losses and found no examples of damage to United States military interests from academic sources.

Second, the governmental effort to control technology transfer is generally diffuse. Many separate agencies are involved, and the effort is spread over many different scientific and technological fields. Enforcement personnel cannot hope to accomplish effective control across all fields. Also, their practical knowledge of the pos-

sible technological applications of these many scientific subfields is limited.

The Panel suggested explicit criteria for narrowing the reach of controls, and encouraged the Government to endorse a strategy of "tall fences around narrow areas." For example, the Panel concluded that the vast majority of university research should be free of controls, and that only in a very small number of gray areas—and that's an extremely small number—may control be appropriate. These are the exceptional cases that Dr. Magrath referred to.

Such gray areas, the Panel argued, must satisfy four criteria concurrently—and these are very strict criteria: One, the technology is developing rapidly and the time from basic science to application is short; two, the technology has identifiable direct military applications, or it is dual-use and involves process or production-related know-how; three, transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and four, the United States is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.

I repeat that all four of these conditions have to be concurrently applied in establishing a gray area.

A third general conclusion was that export control regulations are normally not appropriate tools for the control of scientific communication. Our export control system was assembled to prevent the unwarranted shipment of physical devices, not of knowledge. When control of unclassified research results is necessary, the Government should try to use contractual obligations in funding agreements, not export control regulations. Such contract provisions—stipulating, for instance, that the Government's contract officers concurrently receive for comment materials submitted for publication—provide researchers with relatively clear, advance information on their obligations, in contrast to controls based on export regulations.

I might add that these contractual obligations would still reserve to the university the final decision about publication.

Finally, we need more reliable and complete information about the nature of the overall technology loss problem and the most effective means of staunching it. The Panel was somewhat discouraged at the imprecise understanding of the extent and nature of lost technology, the relative contributions of the many channels by which adversaries acquire Western military technologies, and the adverse effects of control measures.

The Corson Panel report was released in October 1982. There have been some encouraging events since that time. For example, two of the Panel's specific recommendations have been implemented. First, the intelligence community has moved to establish a scientific advisory committee to assist it in reviewing prospective scientific exchange visitors from adversary nations. Second, the Academy itself has established a new Government-university roundtable that will serve as a forum for give-and-take discussions of issues, such as the control of scientific communications, in which there is political conflict between the government and the research communities.

There has also been proposed legislation that drew on the Panel's report. I am pleased that both the Senate and the House have seen fit to incorporate into their proposed revisions of the Export Administration Act the following language:

It is the policy of the United States to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and scholars freely to communicate their research findings by means of publication, teaching, conferences and other forms of scholarly exchange.

This language closely reflects the views of the Panel and other scientific groups on scientific communication, and views that I have expressed earlier.

But these initiatives do not really address the major provisions of the Panel report and will not, of themselves, achieve the major changes that are needed to effect a clear, overall policy.

Shortly after the completion of the Panel study the National Security Council initiated an interagency effort to see if and how the Panel's report could be implemented. The terms of reference for this initiative were set forth in a National Security study directive. An ambitious 2-month completion schedule was set. I am somewhat disappointed that delays have occurred and that for various reasons the administration has not in the course of its review consulted with the outside research community. I understand that the government still hopes to complete its review in the coming months. I am sure that the scientific and university communities would be happy to cooperate, if asked. Moreover, it is important that the results of such a review, when it is completed, be open up and widely communicated.

In any event, I hope the process is a fruitful one. The currently diverse and ad hoc policies are creating considerable apprehension among scientists, who have been and should continue to be active partners in keeping U.S. technology strong.

I recognize that there may be no simple answers to the problems of communications in areas where research is particularly close to military application. However, we should not unthinkingly apply to American science a national strategy of security by secrecy. As Dr. Magrath said, our continuing scientific excellence, and the successful transformation of science into new military technologies of all kinds, depend on extensive dissemination of research results. An alternative national strategy, one of security by scientific accomplishment, by staying ahead of everybody else, has much to recommend it.

Thank you, Mr. Chairman.

[The statement of Dr. Press follows.]

STATEMENT

by

Frank Press
President
National Academy of Sciences

before the
Subcommittee on Courts, Civil Liberties, and
Administration of Justice
Committee on the Judiciary
U.S. House of Representatives

Hearings on 1984: Civil Liberties
and the National Security State

November 3, 1983

My name is Frank Press. I am President of the National Academy of Sciences.

I am pleased to provide my views on a very important national concern -- the relationship between open scientific communication and national security. I became directly concerned with the issue when I was Science Advisor to the President and Director of the Office of Science and Technology Policy during the last Administration. More recently, it was the subject of a major study conducted under the Academy's auspices, by a distinguished panel chaired by Dale Corson, former president of Cornell University. The report of the Corson panel entitled Scientific Communication and National Security was released just over one year ago. Many of my comments today are based on its conclusions.

The subject of this hearing has become a national issue basically because advancing scientific knowledge -- and, more importantly, the technology founded on that knowledge -- has brought two legitimate social objectives into conflict: the advancement of knowledge and the nation's military security.

With the exception of wartime, free international scientific communication rarely has been perceived as detrimental to America's defenses against foreign military adversaries. However, initiatives have been undertaken over the past several years to prevent the dissemination of certain U.S. research results from providing military advantages to America's adversaries. The reaction to these measures has included strong statements of principle both by advocates of scientific freedom and of national security; that is, statements vigorously decrying and supporting such measures.

The issue, in my view, is somewhat paradoxical, for the quality of our new military and commercial technologies derives from U.S. scientific superiority, and that superiority depends upon the open exchange of ideas. The health of the research enterprise depends crucially on scientists building on each others ideas and on the ability to test new ideas against the best existing ideas -- worldwide. The informal exchange of draft scientific papers among leading specialists in the field, travel to scientific meetings and conferences, personnel exchanges, and the publication of papers and their exposure to global scrutiny by other researchers is the essence of productive science. It is, I think, no accident that a nation founded on personal liberties enjoys world leadership in science. And it is no accident that closed societies have

been forced to look outward for the science that must underlie their technological advances.

Thus, American scientists are extremely sensitive to the possibly chilling effects of various recent governmental efforts to control scientific communication. These include attempts to prevent certain unclassified research results from being presented at meetings attended by Russian scientists. That occurred, for example, at a meeting on magnetic bubble devices held by the American Vacuum Society in 1980, at the annual technical symposium of the Society of Photo-Optical Engineers in 1982, and at the Fourth International Conference on Permafrost in 1983. There are also initiatives to require scientists to secure governmental permission before they make their unclassified research results accessible in foreign countries. That would, of course, include virtually all scientific publications, since almost all have an international readership. An example is the "no foreign distribution" condition in some unclassified governmental research contracts.

Perhaps most disquieting, from the point of view of individual U.S. scientists, is that these and other governmental actions to control scientific communication have been largely disjointed, unpredictable, and vague in specifying the scientific fields they are intended to cover. The result is that any particular scientist is

quite unclear about what obligations and sanctions, if any, might apply to her or his work.

More generally, advocates of openness in science point out that imposing national security controls on scientific work may be counterproductive. For example, restrictions on scientific meetings held in the United States may result in international scientific organizations banning meetings in the United States and the relocation of these meetings to other sites that are more accessible to foreign scientists--and less accessible to ours. Also, as the international scientific enterprise continues to advance, the proportion of scientific fields in which U.S. science has a clear lead will diminish -- meaning that international communication in more and more fields will be in our own scientific and technological interest. Finally, there is some danger that in those scientific areas where controls are imposed, some of the best U.S. scientists (and, importantly, some of their best students) will simply transfer their interest to unrestricted research areas, thus depriving military and civilian technologies of their contributions.

Proponents of stricter controls offer arguments that must be seriously evaluated. They point out that, increasingly, U.S. security is related to our technological lead over our military adversaries. The days in which the advantage went to the nation with the

largest military, the best trained soldiers, or the most defensible boundaries are largely behind us. Second, they point out that military technology is, increasingly, what is called "high" technology. That is, more and more critical military technologies are in areas that are very close to current scientific frontiers. In addition, many of these new technologies are "dual-use" technologies -- fields, like advanced electronics, having both military and civilian applications. The significance of the rise of dual-use technology is that one can no longer be certain, even if research is not funded by the military, that it will be irrelevant to military needs.

Citing these trends, those whose job is to protect U.S. national security often point to the danger that we thoughtlessly give away the advantage of our scientific superiority in critical fields.

Both points of view are based on legitimate concerns. The objectives of the Corson Panel study were to consider those concerns, to examine the evidence, and to explore new ways to resolve the dilemma. Major funding support for the work was provided by the Department of Defense, the National Science Foundation, the American Association for the Advancement of Science, and by internal Academy funds reserved for critical national studies. The organization and mission of the Panel on Scientific Communication and National Security was designed to ensure

that it received views from all sides of the issues. Its membership included several former national security officials as well as university and industry scientists. Furthermore, the Panel solicited evidence and differing views of many outside groups.

The Panel in its report, entitled Scientific Communication and National Security, offered 15 specific recommendations. These recommendations rested on four basic findings:

First, although there is substantial evidence of both unwanted transfers of military technologies to the Soviet Union and of Soviet interest in acquiring Western science by both overt and covert means, the Panel found that "in comparison with other channels of technology transfer, open scientific communications involving the research community does not present a material danger from near-term military implications." The Panel carefully evaluated both published and highly classified information on known technology losses, and found no examples of damage to U.S. military interests from academic sources.

Second, the governmental effort to control technology transfer is, generally, diffuse. Many separate agencies are involved, and the effort is spread widely over many scientific and technological fields. Enforcement personnel cannot hope to accomplish effective control across all fields. Also, their knowledge of the possible

applications of particular scientific subfields (to say nothing of knowledge about the relative status of U.S., European, and Soviet progress in each) is also limited.

The Panel suggested explicit criteria for narrowing the reach of controls, and encouraged the government to endorse a strategy of "tall fences around narrow areas". For example, the Panel concluded that the vast majority of university research should be free of controls, and that only in a very small number of "gray areas", may control be appropriate. Such gray areas, the Panel argued must satisfy four criteria:

- The technology is developing rapidly, and the time from basic science to application is short;
- The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;
- Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and
- The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.

Third, export control regulations are normally not appropriate tools for the control of scientific communication. Our export control system was assembled to

prevent the unwarranted shipment of physical devices, not of information. When control of unclassified research results is necessary, the government should try to use contractual obligations in funding agreements, not export control regulations. Such contract provisions -- stipulating, for instance, that the government's contract officers concurrently receive for comment materials submitted for publication -- provide researchers with relatively clear, advance information on their obligations, in contrast to controls based on export regulations.

And fourth, we need more reliable and complete information about the nature of the overall technology loss problem and the most effective means of staunching it. The Panel was somewhat discouraged at the imprecise understanding of the extent and nature of lost technology, the relative contribution of the many channels by which adversaries acquire western military technologies, and the adverse effects of control measures. Obviously, the nation need not fully understand such factors before it moves to stem losses; but in the current situation any control policy is likely to involve unnecessary costs and uncertain benefits. Therefore, the Panel felt the problem as a whole should be further evaluated.

The Corson Panel report was released in October 1982. There have been some encouraging events since.

For example, two of the Panel's specific recommendations have been implemented. First, the intelligence community has moved to establish a scientific advisory committee to assist it in reviewing prospective scientific exchange visitors from adversary nations. Second, the Academy itself has established a new Government-University Round Table that will serve as a forum for give-and-take discussions of areas, such as the control of scientific communications, in which there are conflicts between the government and the research community.

There has also been proposed legislation that drew on the Panel's report. I am pleased that both the Senate and the House have seen fit to incorporate into their proposed revisions of the Export Administration Act the following language: "It is the policy of the United States to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and scholars freely to communicate their research findings by means of publication, teaching, conferences and other forms of scholarly exchange." This language closely reflects the views of the Corson Panel and other scientific groups on scientific communication, views I have expressed earlier. Further, I understand that there has been a constructive series of meetings of a special working group of representatives from the Association of American

Universities and the Department of Defense regarding the formulation of DoD policy.

However, these initiatives do not really address the major provisions of the Panel report, and will not, themselves, achieve the major changes that are needed to effect a clear, overall policy. Shortly after the completion of the Panel study, the National Security Council initiated an interagency effort to see if and how the Panel's report could be implemented. The terms of reference for this initiative were set forth in a National Security Study Directive. An ambitious 2-month completion schedule was set. I am somewhat disappointed that delays have occurred, and that, for various reasons, the Administration has not in the course of its review consulted with the outside research community. I understand that the government still hopes to complete its review in the coming months. I am sure that the scientific community would be happy to cooperate, if asked. Moreover, it is important that the results of such a review when complete be openly and widely communicated.

In any event, I hope the process is a fruitful one. The currently diverse and ad hoc policies are creating considerable apprehension among scientists, who have been, and should continue to be, active partners in keeping U.S. military technology strong.

I recognize that there may be no simple answers to the problems of communications in areas where research is particularly close to military application. However, we should not unthinkingly apply to American science a national strategy of security-by-secrecy. Our continuing scientific excellence -- and the successful transformation of science into new military technologies -- depend on extensive dissemination of research results. An alternative strategy, one of security-by-scientific accomplishment, has much to recommend it.

Mr. Chairman, this completes my prepared statement. I would be most happy to respond to questions from this Subcommittee.

Mr. KASTENMEIER. Thank you, Dr. Press, for that statement.

One of the assumptions, which may or may not be correct, is that recently there is more and more emphasis, if not preoccupation, with research and science in terms of military applications. Now, we all know that surely since 1945 there has been a certain amount of reliance upon and a devotion of resources, scientific and other resources, to military enterprises. But is it your conclusion that recently there has been sort of a step-up in terms of, say, the allocation of resources, research and technology to the military?

Dr. PRESS. The Nation, that is, the Defense Department, is moving to a military strategy that involves the extensive use of advanced technology, in just about every component, every weapon, every device. That, of course, requires a vast expansion in the R&D budget of the Defense Department. With this as a justification, the growth in the Nation's research and development in the military sector has been the largest component of R&D growth in the Federal budget.

Let me say it simply: the R&D growth in the total Federal R&D budget has been led by the military component, with a reduction of the developmental efforts in the civilian sector.

Mr. KASTENMEIER. This reduction in civilian R&D apparently concurrent to that. One of the questions is at what point in time did this take place. Has this been a gradual development? We don't know.

One would assume from what Dr. Magrath said that at least in his view it was about 2½ years, almost coincident with this administration, that this conflict has occurred. Not that the administration alone bears the responsibility, because these are sometimes Congressional decisions. But can we see, in terms of a timeframe, when this new set of problems arose with respect to the governmental supervision of research and the invoking of additional regulations with respect to the flow of information in the scientific field? Is there a point in time this happened, or has this been gradual?

Dr. PRESS. Let me give you my perception, and Dr. Magrath might want to add to that.

I think the current concerns began with the invasion of Afghanistan in the preceding administration. At that time there began restrictions on scientific conferences, reductions in international scientific exchanges, denial of visas and that kind of activity, which has accelerated in recent years as the superpowers have become more and more at odds with each other.

Dr. MAGRATH. Mr. Chairman, I would agree with that. I have to say that obviously my comments are not any more than your inquiry intended in any respect to be partisan, but from where I sit and from where my perspective comes, the kind of problems we are discussing this morning have really surfaced in a very vivid fashion in the last 2 to 3 years. I think that in a sense that does relate to what Dr. Press said about the increasing emphasis on defense research related to military applications.

Now, the previous administration had indicated it was going to support a major defense buildup and expansion. Clearly, it is not controversial to say that that has been a major commitment and emphasis of the current national administration, and if you think

back to Dr. Press' comments about the relationship between this enormous emphasis on applied research related to defense technologies, it is in this period of the last 2 to 3 years that we are seeing this problem intensify.

One of my concerns, if I may just quickly add to that, is that many of us have worked very hard, both in the Government and the Academy and in the major scientific societies, to reestablish healthy linkages between scientists and the Federal Government on the premise that that's in the national interest, and some of the issues we are discussing this morning I fear threaten that relationship and could get us back to the very unproductive tensions that existed in the late 1960's and early 1970's.

Mr. KASTENMEIER. I would agree. In fact, I think Dr. Press, when he said on page 4 that there is some danger that in the scientific areas where controls are imposed come the best U.S. scientists and presumably institutions which simply transfer their interest to unrestricted research areas. They're not going to submit to this sort of supervision, if you want to call it that, in a free and open society.

Well, I have a series of other questions, but I would like at this point to yield to the gentleman from California, Mr. Berman.

Mr. BERMAN. Thank you, Mr. Chairman.

I am interested in your anecdotal story, President Magrath, regarding the Chinese scholar. What kinds of Federal agents came to the university administration?

Dr. MAGRATH. Representative Berman, I did not personally talk with any Federal agents. One of our leading professors of computer science was visited and contacted by agents I believe of the Federal Bureau, the FBI, but I would have to check that. I can certainly provide you specifics on that. That was in the period of 1981 and we certainly had a series of communications and correspondence from the Department of State, which was the initiating agency in terms of those requests that we received.

Mr. BERMAN. You didn't mention the university's response.

Dr. MAGRATH. My response was communicated to the gentlemen in the Department of State in which I said in fairly sharp terms, some sharper terms than I used this morning, some of the points that I made. I indicated we were not going to comply with that.

I then had further correspondence—it is actually published in the appendix to the Corson report that Dr. Press referred to. I indicated that even in terms of releasing certain information, which we weren't in the first place compiling, I would want to have citations of the Federal statutes that justified our releasing such information in view of their conflict with not only Minnesota statutes but also with the Federal privacy legislation.

If the next question is what happened, nothing happened; that is to say, that, in effect, ended the inquiries. I believe the scholar, after about a year or two, transferred to Carnegie-Mellon University. But we did not, in effect, comply with those directives.

Mr. BERMAN. And there was nothing said or done after your—

Dr. MAGRATH. No, sir, not to the best of my knowledge. Nothing happened in the way of overt impositions or restrictions on the University of Minnesota.

Mr. KASTENMEIER. Would the gentleman yield on that point?

Mr. BERMAN. Certainly.

Mr. KASTENMEIER. I thought, Dr. Magrath, you said the University of Minnesota might have been one of five institutions sort of recommended for decertification for certain endowments, if I remember correctly, as a result of perhaps a lack of conforming to certain—or was that in a different context?

Dr. MAGRATH. It was in a somewhat different context, Mr. Chairman. I received, as did, I believe, the presidents of Stanford and Harvard and MIT and possibly Columbia—I can't recall—we received a communication from a private, not a governmental, but a private individual. I think that has to be made very clear.

Mr. KASTENMEIER. That's correct. You did say private.

Dr. MAGRATH. It was telling us, because there had been some publicity about various positions that those universities had taken on these questions, that we, in effect, were not acting in the national interest and that this group was going to pursue shareholder resolutions at corporate meetings to discourage these corporations and foundations from making grants to the universities that were not collaborating with the national interest.

I have to say we do occasionally have concerns that the positions we take might cause us difficulty, but in fairness I have to say I have as of yet seen no evidence of that fortunately, and I hope that will never happen.

Mr. BERMAN. That threatened blacklisting never took place, I take it.

Dr. MAGRATH. Well, of course, we all believe in the fifth amendment, so nothing bad has happened yet that I'm aware of. It's possible that there were some enormous grants that some corporation was going to give us that we didn't get, but I don't think so, no. I don't think anything has happened. I just think we do run the risk, whenever we take this fairly clear position, that we irritate those who define the national security interest in a certain way.

Mr. BERMAN. Do you think in this particular situation that the actions, threatened actions, or the comments of these managers of these private foundations were induced by governmental pressure?

Dr. MAGRATH. Mr. Chairman, Representative Berman, no, I do not. I see no evidence of that.

Mr. BERMAN. So there is not really much they can do in this area.

Dr. MAGRATH. No, I see no linkage, sir.

Mr. BERMAN. You mentioned the fuzziness of the Export Administration Act regulations in this area. Is it possible to amplify that? The reason I say that is, as Dr. Press pointed out, we made a very generalized and nonspecific statement—I'm on that committee and was very involved in that bill, which just passed the House and which will be going to the conference committee at some point in the near future. We passed and I guess the Senate passed, although I'm now advised that there is a very major difference in how the report language construes the exact same words in the bill that both the House and presumably the Senate very soon will be passing, a very generalized kind of language that was read in Dr. Press' statement.

If it would be possible to get some sense of the regulations that perhaps were overbroad or stifling or struck an improper balance

between these competing interests, if only there could be a very quick congressional remedy perhaps to that just in the context of finishing up work on that bill, I was wondering if you could comment on some of those specifics.

Dr. MAGRATH. Maybe, Mr. Berman, Dr. Press can help me with that answer. It is my understanding that there are clarifications moving in Congress that would be helpful in resolving the ambiguity. The fundamental problem, as I understand it, is that the regulations are so broad that—universities are in the export business, in the sense of the exchange of ideas. This is discussed at some length in the so-called Corson Report and maybe Dr. Press could comment on that further in response to your question.

Dr. PRESS. I would have two suggestions. The language that amplifies the need for open scientific communication as a prerequisite for maintaining our position as the world's leading scientific nation appears in the report to the bill rather than in the bill itself. It is my understanding that executive agencies feel they are not necessarily bound by report language, although that is a continuing issue of discussion between Congress and the executive branch.

Second, the Senate version contains the vague statement that restrictions on scientific communication should be avoided except when overriding national security concerns must appropriately take precedence. That's a very vague statement that can be interpreted in so many different ways by so many levels of bureaucracy in the executive branch that I fear it could prove an escape clause that might be invoked too often.

Mr. BERMAN. That's in the Senate report language?

Dr. PRESS. Yes.

Mr. BERMAN. You mentioned, Dr. Press, the general conclusion of the panel that all in all, when we talk about the hemorrhaging of technology and acknowledge that information has been received by the Soviets from American sources that it would have been best they had not received from a national security point of view, that it is also the panel's view that the research activities and communications of scientists in these international forums and exchanges is a negligible part of that problem.

Now, every business community in the Export Administration Act hearings said they're a negligible part of the problem. Where is the problem?

Dr. PRESS. I think there has been a damaging flow of technology to the Soviet Union consisting of hardware that is immediately usable or applicable in the near term in Soviet military systems. It has come from illegal industrial sales, third country sales, espionage, industrial espionage. That has happened. But it has not come from the kind of scientific communication, the publications, the teaching, the international exchanges, that are the hallmark of a research university. That has not been the source of this damage.

Mr. BERMAN. Thank you very much, Mr. Chairman. I yield back.

Mr. KASTENMEIER. That was an illuminating answer.

You indicated, Dr. Press, that the Corson Panel had stated that four criteria ought to apply, and apply in concert. Do I understand that these criteria have not yet been accepted by the administration but that the administration is still considering them? Is that the correct state of affairs?

Dr. PRESS. The administration deliberations are closely held, so I just don't know what the progress is and to what extent they are following these recommendations. I do know that the Corson report is being used in the administration deliberations as input to their discussions, but how the policy is evolving in the internal administration discussions is not known to me, nor to anyone else on the outside.

Dr. MAGRATH That's correct. We don't know what the answer is, in effect.

Mr. KASTENMEIER. Dr. Magrath, in terms of the four criteria, are you satisfied that they are sufficient?

Dr. MAGRATH Yes, sir. I wouldn't presume to speak for individual faculty members at the University of Minnesota. I have been around too long to do that. But from my own perspective, because I know the authors of the report and what they intend, I can live with and see the reasonableness of those criteria. But to reemphasize, it's a gray area but it is not a big, broad gray area as it is stated. It is a very narrow gray area.

Dr. PRESS. And it is also a gray area that would require a dialog for 60 days but would not lead to a prohibition of publication. That's a key point.

Mr. KASTENMEIER. Some critics of the Corson report say that the report in a sense asks the wrong questions or possibly assumes the wrong premises, insofar as it merely attempts to accommodate security concerns of the intelligence agencies and the military rather than the other concerns, such as preserving openness and traditional academic freedoms. Do you have any comment on that?

Dr. PRESS. Well, having spent 23-some-odd years in the university, and 4 years in the Government, I think I appreciate the concerns on both sides. I think, not because the Corson report comes from my own institution, but I think it was an extremely balanced statement, taking into account the legitimate concerns of both the Government and university community.

It is an eloquent statement of the need for open universities and free scientific communication, as eloquent as I have seen.

Mr. KASTENMEIER. Others are concerned that the part of the Corson report in which it appears to premise the assessment of the nature of the problem is really based on a classified report, which is not made public. Apparently, the classified report proved that technology transfer was a significant problem, but insofar as this is not available for general review, can it have full credibility?

Dr. PRESS. Mr. Chairman, there was no classified report. The Corson report was the—well, let me see. I had better back off. There was—

Mr. KASTENMEIER. I'm not talking about the report itself.

Dr. MAGRATH I think the reference is to some of the information that was made available to the Panel.

Dr. PRESS. Yes. Let me back off—

Mr. KASTENMEIER. Which in the beginning made its assessment of the nature of the problem.

Dr. PRESS. It has been a year or more and now it's coming back to me. A subcommittee of the Panel received briefings that were classified. These were briefings by the intelligence agencies about the kinds of damage that has occurred by American technology.

showing up in Soviet military systems. These were briefings about the sources of this technology leakage—industry, espionage, third-country transfers, universities, and so on.

As a result of those briefings, the subcommittee concluded that open scientific communication was not the source of this damaging technology transfer, but the sources were the other sectors that I described to you. There was a written statement that was classified that summarized those briefings.

Mr. KASTENMEIER. If that was the case—and for the record I'm arguing the point in the sense of trying to explore the situation—why would then conclusions be reached which would, say, be more permissive of the Government limiting universities when they are not the source of the problem? And maybe you don't read the Corson report that way.

Dr. PRESS. No. The proposals, the so-called limitations of universities, are no more severe than the universities impose upon themselves for such things as patent protection, and no more severe than the universities impose upon themselves in dealing with industrial sponsors of research. Universities insist that there not be an undue delay in publication, no more than 30 or 60 days. The universities insist that their openness—their teaching and freedom to communicate—not be compromised in their own privately sponsored research. The Corson Panel recommends limitations no more severe than that, and then only if very strict criteria apply. The Corson report recommends only a 60-day delay in publication so that the Government contracting officials can discuss particular paragraphs in a report with the researchers that they sponsor. The universities have the final right of decision in the recommendations. So, it is not a proposal for something that is extraordinary in academic life.

Mr. KASTENMEIER. What does it say with respect to the number of things that President Magrath detailed as problems for the scientific and academic community?

Dr. PRESS. I would say that as I listened to President Magrath's talk I could subscribe to just about everything he said. In fact, I can't think of a single exception, although I would like to read his statement over again. But I was just nodding my head all the time that he was making his presentation.

Mr. KASTENMEIER. The point is, there seems to be some slippage between what is actually happening in the country and, say, the Corson report, or that which is complained about.

Dr. PRESS. I see what you mean. The Corson report is a recommendation from a private sector organization, the National Academy of Sciences, to the Government. It is not a requirement on the Government by any stretch of the imagination. It has no force of authority. It is just a private organization's view, an organization with a traditional relationship to the Government, but these are policy recommendations that the Government can act on or not, as it sees fit.

The fact that there have been scientific meetings where papers were forced to be withdrawn, the fact that there have been a number of instances of the kind that you heard, concerning foreign students on the campuses, some instances even more severe than

what you just heard, these are ongoing problems that we have to address.

Mr. KASTENMEIER. Is it not a concern to people in the administration that there is growing—perhaps hostility is an overstatement—but tension surely between the scientific and academic community and the regulations and other restrictions imposed by the administration on them? Are they not aware of it, or do they feel that the overriding need for national security considerations are such that they must proceed irrespective of the feelings of the community?

Dr. PRESS. It is very difficult for me to characterize the administration's concerns, especially when the discussions are private. But I would venture a guess that the senior administration officials in science and technology are very sympathetic with the Corson Panel report. The reason for that is that they understand the nature of scientific discovery and technological innovation. They know that once you start compartmentalizing science, then you start degrading scientific productivity. They don't want to see that happen—for the benefit of the country. So, by and large, I would say they are sympathetic.

I think the problems we have come from those in the administration who don't have such experience and who tend to lump basic science and advanced technological hardware together, without understanding that they are quite different.

Mr. KASTENMEIER. Of course, it is not the scientific adviser or people that you referred to who are really in control in terms of regulations and directives that are issued.

Dr. PRESS. Having had that position, I would say that the Presidential science adviser is one of many voices and many different points of view that will be considered in the final decisionmaking process.

Mr. KASTENMEIER. Dr. Magrath.

Dr. MAGRATH. Just a brief comment, Mr. Chairman.

Dr. Press is much closer and far better qualified to answer the question that you posed to him, but my sense of it is that his comments are exactly accurate and that there are persons and voices within DOD and elsewhere within the Federal Government who are very sympathetic to the position that we are taking. But there are other voices and other points of view as well.

I would also like to say this is the Corson report and I did not serve on the Panel, although I believe I was invited to and couldn't. I believe that while I'm sure one can find points of difference here and there, I think we can study and discuss and debate these very difficult issues for many weeks and months and I don't think you will find a better statement of the problem, and a stronger affirmation of scientific and academic freedom, and a more sensible set of recommendations put together in a period of I think 3 or 4 months, by some very hard-working individuals, than in this document. It's as good a guideline I think as we could have, as Congress and you and others explore these very important issues.

Mr. KASTENMEIER. Apparently it is not being followed, and our problems are that decisions are being made by others who do not give the highest priority to those considerations.

Coming from the scientific area and the educational area, I happen to believe that these two fields have a great deal to do for our national security beyond our military strength. So I think we have to take a broad view of what constitutes national security.

Within this context, I think that any restriction of science, of the kind we have been speaking about, would start us down the road of losing our scientific preeminence in the world, which I think is a very important element of our future national military security, national economic security, and the cultural life of the Nation.

Mr. KASTENMEIER. Thank you.

Mr. BERMAN, any further questions?

Mr. BERMAN. Just a couple.

In your testimony, Dr. Press, this reference to the "dual use" capabilities, you cite several instances where apparently there have been administration efforts to prevent certain unclassified research results from being presented at meetings attended by Russian scientists. I am just not informed at all on the nature of these and have no scientific background.

One of them is the Society of Photo-Optical Engineers in 1982. Somehow that strikes me as spy satellites or technology that might be used there. Am I just totally off base or is that—

Dr. PRESS. No. Photo-optical devices are a very important element of many different military systems. I am sure there is a legitimate need in certain areas of that technology, where the military application is obvious, to examine it from the point of view of classification.

But it is also a field that is extremely important in civil technologies, that are in use today such as optical communication systems—which replace copper with optical fibers—and the laser devices for phonograph playback and high-fidelity recordings. There are all sorts of new devices based upon photo-optical technologies. So it is a very big, economically important field, with some military applications.

If we are going to achieve commercial strength in this country in this very important field, we have to have open communication in scientific meetings. But again, I think if there is a case for classification, the rationale it should be made and should be made very clear and very specific, and people should know about it.

Mr. BERMAN. But how do you make—

Dr. PRESS. When one organizes a scientific meeting and all of the papers are received, and they are all unclassified, and then 2 weeks before the meeting there is an order saying "These papers have to be withdrawn because you're liable for prosecution under the Export Administration regulations" that's not the way to have open scientific communication. It alienates the scientific community and it encourages international scientific bodies to have meetings outside the United States.

Mr. BERMAN. How do you—I'm asking these questions because I can think of people in this body whose initial reaction to this kind of discussion is, well, how do you know that the papers that are going to be delivered relating to the cutting edge of research in this area are, in fact—even though they're not done by the Department of Defense or under the sponsorship of the Department of Defense, and may be much more a product of academic or research or re-

search under some private foundation contract—are so revealing that a level of information will pass into the hands of the Soviets in this kind of exchange, that there should be some prepublication review or a potential to stamp on to that document classified, or at least classified as to foreigners or classified as to Soviet scientists.

What is the process?

Dr. PRESS. As I understand it, except for atomic energy, the Government has the right to classify only those things that it pays for. So we're talking about Government contracts for research. Those contracts for research with universities are carefully defined, carefully spelled out, and with all research universities they are unclassified contracts or else the universities would not accept them. So there is a clear charge to the researcher, or there is a clear proposal by the researcher—"I will work in these fields, and this is what I intend to do."

Almost all of the time that work stays on the unclassified side. Once in a very rare experiment, a very rare result, the university researcher may walk across a line where his research becomes useful in the very near term in a military system. There might be a justification for classification at that time.

The process we have, and it's a good one, is that the Government contract official usually knows what's going on on the university campus. There are progress reports that are made, there is communication, and most of the time that excursion into the classified area is recognized by both sides.

At that point there is a decision to be made. The Government can classify it, in which case the university will stop doing that research—to the detriment of the Government—or the Government will take its chances and not classify it because it becomes very excited about its potential. But there are mechanisms and means for doing these things.

The problem is with research mutually agreed to be unclassified. A new category is being invented ad hoc when the Government takes unclassified research and treats it as if it were classified by prohibiting its presentation.

Mr. BERMAN. The last question I have is for Professor Magrath.

Some people apparently, including Admiral Inman, have argued that the type of prepublication review urged by the executive branch is virtually parallel to that imposed on researchers supported by corporate funds, and apparently accepted by those researchers. You may have touched on this in your answer to the chairman's question, but I would just throw that out.

Dr. MAGRATH. Well, Mr. Berman, I can't speak for other universities, but I know that at the University of Minnesota we do not—and we have some very close linkages with industrial firms and corporations—we do not and will not agree to prepublication restrictions. Most of the relationships that I'm familiar with at least, involving research universities and corporations, are very much within the traditions that, generally speaking, historically have worked well between universities and the Federal Government. In fact, I happen to believe that there are many good models that historically have existed between the Federal Government and university researchers and that they are part of the answer to some very difficult questions involving corporate-university relationships. But

we would not agree to prepublication agreements that in any way are different from the kind of situation that Dr. Press has outlined.

Mr. BERMAN. Thank you very much.

Mr. KASTENMEIER. The committee wants to thank you both for your contributions, Dr. Press and Dr. Magrath. It has been very helpful and very informative for us and contributes—not only your presentations but your answers to our questions—to our understanding of the problem and hopefully to the public discussion that we trust will ensue.

Dr. MAGRATH. Thank you, sir.

Dr. PRESS. Thank you very much.

Mr. KASTENMEIER. Our next witnesses will make their presentation as a panel. The first member of the panel is Prof. George Davida of the University of Wisconsin at Milwaukee. He is an expert in matters relating to computer science in general and cryptography in particular. He has had some personal experience relating to restrictions on the publication of scientific information.

Our second witnesses represent the Institute of Electrical and Electronic Engineers. IEEE is a national professional organization that frequently sponsors scientific conferences and exchanges. Representing IEEE will be Professor Karl Willenbrock from Southern Methodist University. Accompanying Professor Willenbrock is Ellis Rubenstein, managing editor of the organization's magazine "Spectrum." Mr. Rubenstein will relate his testimony of personal experience with attempted restrictions on publication by the Department of Defense.

The final member of our distinguished panel is Prof. Stephen Unger of Columbia University. Professor Unger is also an expert in computer sciences and has been actively involved in the subject on a number of panels of the American Association of University Professors, the AAAS, and has also written extensively on the subject of academic freedom.

Gentlemen, you may proceed. Professor Davida, you may proceed first.

Professor DAVIDA. Mr. Chairman, I would just like to refer to my report.

Mr. KASTENMEIER. Without objection, your statement will be received and made a part of the record, and you may proceed as you wish, professor.

TESTIMONY OF PROF. GEORGE I. DAVIDA, DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, UNIVERSITY OF WISCONSIN-MILWAUKEE; PROF. F. KARL WILLENBROCK, CHAIRMAN, IEEE TECHNOLOGY TRANSFER COMMITTEE, ACCOMPANIED BY ELLIS RUBENSTEIN, MANAGING EDITOR, "IEEE SPECTRUM"; AND PROF. STEPHEN H. UNGER, COMPUTER SCIENCE DEPARTMENT, COLUMBIA UNIVERSITY

Professor DAVIDA. Thank you, Mr. Chairman.

My own experience with the Government's classification powers occurred in 1977 and 1978. We had been funded at the time by the National Science Foundation, in one of those grants that was referred to earlier by Drs. Press and Magrath. It is an unclassified research grant, although my understanding is that a lot of the

award letters that are being issued now are being perhaps tightened up to allow possibilities of classification even under NSF-sponsored proposals.

But, in any case, in 1978, as a result of a patent application, we were issued a secrecy order that, among other things, contained penalties of 2 years in jail and \$10,000 fine for unauthorized disclosure of a subject matter we had invented on our own, without any reference to classified information. What that seems to imply, Mr. Chairman, is that there are some things that some regard as being born secret—in other words, regardless of how you arrive at them, somehow you cannot disclose them.

I don't know how these concepts came about to be accepted by some, but I do find them to be contrary to the principles of this country. I don't accept them. I don't know about my other colleagues, but I don't think we should be subscribing to the theory that there is some knowledge that simply cannot be talked about.

Now, the problem that I see really is twofold: what is the impact of the classification powers of the Government, and will it, in fact, achieve the desired effect of denying our adversaries the fruits of our labor?

When one considers other models of secrecy that we practice in this country, I'm not entirely convinced, Mr. Chairman, that secrecy has really done a lot for us. I have asked physicists who worked on nuclear weapons whether the secrecy they practice has, in fact, prevented any country from introducing a nuclear weapon if it had the resources. The answer has always been that it has not. In other words, the research that is being conducted and the secrecy that is being practiced in areas where there is effective control, not only is the transfer of technology not necessarily as controlled as we would like, the results are not exactly all that encouraging.

In the nuclear weapons industry, I understand that people in the highest levels of Government seem to say that we're either at about the same level in terms of destructive capacity as the Soviets, or that they are slightly ahead. If that's the case, I would hate to see what would happen to our other technological advances in non-DOD areas. Perhaps if we practiced secrecy we would be just as mediocre as the Soviets.

It is clear that secrecy appears to have nothing really in store for us except mediocrity. I don't think that we will in any way keep our lead or even make advances if we continue on this path of restricting the flow of information among the scientists.

Now, there are some other issues that this business of classification brings up. I remember when we first received the secrecy order, one of my colleagues came up to me and said that we should be honored that our research was classified. In other words, there was a tendency on the part of some to think that if the research is classified it was important. I would hate to see that kind of thinking creep into the academic process.

For example, in one case, it is my understanding, one of the Government agencies that was interested in some of the research actually interceded on behalf of a faculty member, I guess writing some kind of a letter to his department chairman or somebody, in effect telling the institution that his work was so important that that person ought to perhaps be granted tenure. I don't wish to see such

involvement of Government agencies, particularly intelligence agencies, in the issues of academic freedom and issues of tenure and the publication of our results. I think that would obviously be contrary to the way we do research at universities and not in any way enhance our research capabilities.

Finally, I do think that the Government has the obligation to be consistent. On the one hand, we do have exchanges with our adversaries. We sell them all kinds of products, food and other technologies, and at the same time the Government turns around and tells us that we should not communicate among ourselves to prevent the Soviets from learning what we know.

If I may summarize, the Government must get its act together. I find the current regulations, both export control regulations as well as the secrecy act, to be rather confusing, and chilling. I don't think that we can live with the kinds of vagueness that has been referred to by others. With that I would like to conclude, Mr. Chairman.

[The statement of Professor Davida follows:]

Testimony before the Subcommittee on Courts, Civil Liberties and
the Administration of Justice

November 3, 1983

Professor George I. Davida
Department of Electrical Engineering and Computer Science
University of Wisconsin-Milwaukee
Milwaukee, WI 53201

In 1977 the Wisconsin Alumni Research Foundation filed for a patent on behalf of myself and a graduate student for a data protection device that resulted from research funded by the National Science Foundation. The research was unclassified and was based on materials publicly available. In 1978 we were issued a secrecy order by the Commerce Department which, unknown to us at the time, had done so at the request of the National Security Agency.

Upon careful reading of the secrecy order, we became concerned since the order contained penalties of two years in jail and \$10,000 fine for unauthorized disclosure of the subject matter of the patent application, which, I would like to emphasize, was based on publicly available material.

Upon informing the University of the secrecy order, the Chancellor became quite concerned that the order infringed on academic freedom, not to mention the First Amendment. After the resulting press coverage, the Chancellor communicated with the then Commerce Secretary Krepps and NSA director Admiral Bobby Inman. A short time later, the order was rescinded.

In 1979 the American Council on Education undertook a study of the issue of publication of research in Cryptography and its relation to national security. The group, called the Public Cryptography Study Group (PCSG), met for about two years and in 1981 issued a report in which the majority of the members recommended a system of "voluntary" prior review. I dissented from this recommendation and issued a minority report in which I outlined my reasons for opposing what I saw as nothing more than

ensorship.

My opinion has not changed. I still oppose the system of prior review. My concern has grown as I have seen my predictions, that the government's interest in classification of research would grow to include other areas, come true.

The secrecy orders and the PCSG's recommendations raised issues that had a direct bearing on the Nation's political, scientific and economic health. More specifically, the secrecy orders and prior review raised questions regarding:

1. Constitutionality

The secrecy order that was issued to us was for material that we had discovered without knowledge of classified information. The government seemed to regard this subject to be what some have called "born secret." Such concepts have no place in our democracy.

2. Impact on Basic and Applied Research

Secrecy orders and censorship of results deemed by some in the government to be a danger to the national security would inevitably lead to the removal from the public domain of interesting results. There is no doubt that this would seriously harm the quality and direction of research.

The PCSG's recommendations were equally disturbing. It was without any basis since the committee had no evidence to suggest that publications in cryptography were harmful to the nation's security. The committee did not consider the critical importance

of cryptography in data protection. Our nation is changing. The most intimate details of our lives are being stored and manipulated by computers. Medical databases, credit files, insurance files, employment records are being constructed and connected to computer networks. The increased use of personal computers may lead to personal databases. These technological changes can potentially destroy not just privacy, which is already gravely threatened, but freedom itself. It is difficult to conceive of freedom without privacy. We must be allowed develop the technology to protect information that we do not wish to share with others.

Economically, our society is changing in such a way that our assets are no longer physical, but logical. Disks and not vaults are the repository for the new wealth. Wealth is being reduced to just "bits" and "bytes" in some computer. Electronic funds transfer would make it possible to move this wealth at unprecedented speeds.

The need for protection technology was made abundantly clear in the reported Soviet evesdropping activities. More recently young computer buffs raided computer systems all over the country. What caused these weaknesses? In the case of cryptography, the government would not only not share its knowledge in data protection, but was now attempting to suppress information developed in the civilian sector. These actions clearly indicate that the blame for the vulnerabilities in our communication and computer systems rests with the government.

3. Effectiveness of Such Measures

Even if one was willing to ignore all the other objections to suppression of information, there still remained the question of whether the actions would have the desired effect of denying the results to our enemies. There is no evidence that there is significant contribution to technology transfer to our enemies by publications of basic research. Studies have shown that technology transfer to our adversaries occurs through commercial exports from both the United States, Western Europe and Japan. What little impact from publications there may be has to be balanced against the obvious benefits that this nation enjoys in just about every area of technology that we choose to pursue. We are clearly the world leaders in those areas that we are equipped to conduct research in. There are areas in which, some say, we are losing our lead to, not the Soviets, but the Japanese. The decline of investment in research has been well documented. It, therefore, should not surprise anyone if we lose our lead in areas that are underfunded. Our shortcomings are not due to lack of ability. Our problems have been the lack of national leadership to reinstate the resources necessary to maintain (or regain) our technological lead.

In assessing our technological strengths and weaknesses, some comparisons are in order. Just how well are we doing compared to, say, the Soviets? It is interesting to note that in the non-defense R&D and production, we are clearly decades ahead of the Soviet Union. But when we consider nuclear weapons, government officials at the highest levels tell us that the

Soviets are either equal to us (the prevailing view) or are slightly ahead. It thus appears that in an area where both we and the Soviets practice secrecy, the results are about the same! This is rather strange since one would expect that, in a field where we were practicing secrecy and thus denying the Soviets the opportunity to share in our advances, we would be ahead given our overall lead in technology. This implies that if we were to impose secrecy in other areas of engineering and science then what we can expect is that we will do about as well as the Soviets. Secrecy, it seems, has only thing one in store for us: mediocrity.

It is also possible that if efforts to restrict the flow of information continue, then not only will they damage our research capability, but may very well start an "information war" with our friends.

Finally I, like many others, am concerned about the inconsistency of my government's actions. The government sells the Russians wheat to help feed them and then turns around and tells us that we must not communicate among ourselves lest we help the Russians. Apparently the government believes that it can better protect us from the Russians if it keeps the Russian stomachs full and our minds empty.

Mr. KASTENMEIER. Thank you.

Next I would like to call on Dr. Karl Willenbrock. We have your 13-page statement and you may proceed from it, or summarize it, if you wish.

Professor WILLENBROCK. With your permission, Mr. Chairman, I would like to submit my statement for the record and summarize my comments.

Mr. KASTENMEIER. Without objection.

Professor WILLENBROCK. First I would like to make a few comments about the scientific and engineering professional societies in general, and IEEE in particular, since the incidents I will be describing are those related to the Institute of Electronics Engineers.

This Institute is a leading professional society for the electrical, electronics and computer engineers and scientists. It has a transnational membership of more than 230,000 members. It has roughly 190,000 members living in the United States. It publishes more than 50 technical periodicals and it sponsors more than 225 major technical meetings on a yearly basis. It is a very active and dynamic group.

It is typical of many of the professional societies that exist in other areas of technical specialization. There are more than a thousand such societies in the engineering and scientific areas throughout the country. It is a safe generalization to say that there are no major areas of science and technology that are not served by an active professional society.

The important point I would like to make, and it is reinforced by the statements made by the previous testifiers, that the meetings and periodicals really are an integral part of the communications system that was described in more general terms by Doctors Magrath and Press. The papers presented are presented for the information and stimulation of the technical community. The people that participate are from all parts of the spectrum. They range from Nobel Laureates to students. Such presentations are an effective and important part of the communication which keeps the community alive. People go to the meetings and read the periodicals to know what is going on in their fields. It is the way of maintaining and keeping up to date fast-moving technological areas.

If I may cite a personal experience, last summer I spent a few weeks in Indonesia as part of a U.S. group working with their Ministry of Research and Technology. The Indonesians are very interested in improving their rate of scientific and technical progress. I was amazed to find that there is very little professional society activity there. Scientists and engineers from different groups really did not know what was going on in their own country. It is not surprising that their rate of technological progress is quite slow. I feel, as do most members of the scientific and technical community that our open system is a very integral part of what makes us move ahead rapidly. It has been an essential element contributing to the leading worldwide position that the United States now has in science and technology.

Let me now discuss the openness of the system and answer a question that was raised by previous witnesses. How open is the system? What about proprietary information in the industrial community?

The communication or information dissemination system is as open as people want to make it. There are some pressures both ways. Look at it from an individual standpoint. An individual would like to present his research results and get the acknowledgment from the community of his peers. On the other hand, most researchers don't give away what they plan to work on next because they don't want to be scooped. People make individual judgments as to the content of their presentations. This is particularly true for the university community.

Now consider the industrial community. Engineers and scientists in the industrial community typically have their papers reviewed by their patent departments. They are concerned about giving away commercially important information. However, most companies have learned how to do it; they keep proprietary information out of their papers, but still their engineers and scientists are active participants in the communication process. Look at the IEEE as a typical organization. More than 60 percent of its authors are industrially employed. In some ways the company has some of the same motivations as the individual. Companies want to be considered first-class technical organizations that are up-to-date. They are active supporters of the professional societies. Their employees are members and participate actively in both the meetings and the operation of the periodicals. There are ways for individuals to operate effectively with some information which is not open and other information which is open. Industrially-employed engineers as well as the university-based engineers operate very effectively together.

Some of the problem areas have been illustrated by the previous speakers. It should be understood that there really aren't procedural problems related to information which is clearly assigned a security classification by the appropriate government authority. Such information is not published in IEEE publications or presented at open IEEE meetings. It is IEEE policy to require all authors to certify that the papers they submit for publication or presentation at meetings have been cleared by the appropriate authorities within their organizations.

Difficulties arise when authors submit for publication or presentation information which is considered releasable or has been released within their companies, but then is later described as classified or otherwise unpublishable by a Federal agency representative.

Let me cite three instances in which the IEEE was directly involved.

The first incident involves an article which was submitted by an author for publication in the IEEE Spectrum last year. Spectrum is an award-winning monthly periodical which is circulated worldwide to all IEEE members. Accompanying me today is Mr. Rubenstein, the managing editor of Spectrum. He was directly involved in the incident. He can supply more detailed information if you so desire.

The article was entitled "Out-Numbered and Out-Weaponed by Soviets, the U.S. Army Shoots for High Technology," and after being submitted by an external author, it was subjected to the usual expert review process. Since the author quoted the then Secretary of the Army, the article was sent to his office for review. A

month-and-a-half later the Spectrum staff editors received a telephone call from the Army Office of the Chief of Public Affairs with the message that the manuscript contained classified information and should be shredded immediately.

Upon questioning, the Army representative identified three statements as being classified. The Spectrum staff investigated the origins of these three statements and found that two statements had been published in an unclassified, widely disseminated Army publication entitled, "1982 Weapons Systems," and the third was from public testimony of the Army Chief of Staff to the 97th Congress.

When this information was presented to the Army representative, it was agreed that the two published phrases were not really classified but that the Chief of Staff's testimony had been reclassified. The explanation was offered that unclassified information can sometimes be put together in such a way as to be reclassifiable. It turns out that this issue was not pursued further, since the article did not meet the technical standards appropriate for the Spectrum. The article was not published.

However, the incident does provide an opportunity to examine the effect that such Federal agency actions can have on the scientific and technical publishing community. Many authors of technical articles confronted with such a statement by a military representative would simply have withdrawn the article. However, in this case a full-time editor of Spectrum who is not readily turned aside followed up and found that the reasons for withdrawal were at best questionable. Many technical authors—and I would consider Dr. Davida as an exception—tend to avoid topics that might be disapproved by a Federal agency. They try to keep out of harm's way and try to avoid getting involved with such issues.

Mr. KASTENMEIER. Dr. Willenbrock, regrettably I am going to have to interrupt the remainder of your presentation so that we can make a vote on the House floor. That's what the buzzers were all about. Therefore, we will have to recess for 10 minutes. I regret dividing your very fascinating testimony, but if you don't mind, sir, and the other witnesses, we will have to recess for about 10 minutes. We will reconvene at about 12:15.

Accordingly, the committee is in recess.

[Whereupon, the subcommittee was in recess.]

Mr. KASTENMEIER. The committee will come to order. We will return to Dr. Willenbrock, who was in the middle of his presentation.

Professor WILLENBROCK. Thank you very much, Mr. Chairman. Your timing was good enough to interrupt between incidents one and two.

The second incident happened last year in connection with an IEEE-sponsored International Test Conference in Philadelphia which was run by the IEEE Computer Society.

Five days before the conference was to open, and after the conference publication had been printed, an official of Texas Instruments, Inc. requested by telephone that three papers written by TI engineers on very large scale integrated circuits be withdrawn. The Air Force Systems Command considered the release of these papers to be potentially damaging to U.S. interests. The authors, who are

IEEE members, believed their papers were cleared having followed the usual internal procedures at TI.

Apparently the government reviewers did not decide until very late—that is, until 5 days before the conference, after the Conference Digest had been printed and some copies supplied to reporters—that the papers should not be published. The conference managers were asked to excise the papers from the already printed Conference Digest and to ask reporters who had received prepublication copies to return them.

The conference managers decided to require before taking these steps that: One, a written explanation of the reasons for removing the papers be given; two, that the authors themselves request the removal, and three, that an agreement be made to pay the costs of destroying portions of the already printed record. In response to these requirements, a rereview of the papers by the Air Force resulted in a decision that the original papers could be presented as planned. They were.

A third incident occurred in 1982 in connection with the EASCON Conference held in Washington. It was sponsored by the IEEE Aerospace and Electronic Systems Society. Just before the conference opened the conference chairman was asked by an Air Force representative to destroy all conference records and to cancel the presentation of certain papers. The conference chairman responded that he might agree to do so if the estimated cost of between \$25,000 to \$50,000 was borne by the Air Force. A day later, the Air Force representative withdrew his request. Later a Navy representative made a similar request which was also withdrawn after the costs were described.

In view of these incidents, it has become evident to the IEEE that it needed to have a practical procedure to handle such cases. Typically the chairman of an IEEE Technical Conference Program is an engineer employed by a company or university who undertakes this additional responsibility as a part-time voluntary professional society task. The IEEE is presently working on what we call a hot line procedure which would make available to any conference program manager or journal editor access to the IEEE general manager's office. In this office, previous experience with this type of situation is available and also legal counsel is available if necessary. We are also seeking to develop appropriate points of contact within the DOD so that reasonable decisions can be reached in short periods of time.

The IEEE does not have a complete record of how many incidents of this type have occurred, since they are not all reported. However, there have been other incidents in which papers have been withdrawn at the request of military representatives.

I might interpolate that the general advice that is given to IEEE representatives in such cases is that, first, don't roll over, second, get good advice, and third, don't go to jail.

It is difficult, if not impossible, to measure the impact on the electrical/electronics and computer community of incidents such as these. Certainly they have the chilling effect which was described by previous testifiers. I should like to cite two examples of such effects, one relating to an IEEE committee, and the second relating

to the research choices of an IEEE member who is a very capable junior engineering faculty member.

A number of IEEE members who are part of the Solid-State Circuits and Technology Committee canvassed their members recently to determine what topics would generate the most interest as focal points for proposed workshops in the spring of 1982. Two topics were selected, one on high speed technologies and the other on the very high speed integrated circuits program, VHSIC, which the DOD has sponsored.

Before going ahead with planning for a workshop on VHSIC, the DOD program manager's office was contacted. The manager's representative indicated that VHSIC was controlled by the international traffic in arms regulations [ITAR]. Therefore, if the workshop included information on chip fabrication and processes, chip architecture, internal details of the chip, and the performance details of chips, all workshop attendees would be required to present proof of U.S. citizenship. Such proof would not be required if only topics such as brass boards and the names of chips were to be covered.

The IEEE group decided that there were too many constraints and the result was that this workshop was not held. Whether this decision was an advance or a loss for U.S. national security is hard to decide. However, it is possible to assert that the planners of this workshop, which included engineers from Bell Labs, IBM, and the University of California at Berkeley, et cetera, are among the most productive and capable engineers in the United States in this particular field.

The second incident I would like to relate is a personal experience with a fellow faculty member at SMU, who recently completed his Ph.D. at Princeton in communications theory. We were discussing some of the interesting areas where technical problems existed, and he indicated he carefully avoided those topics which were close to DOD interests because he feared his work could be classified. He considered this possibility disastrous because it would not enable him to publish his results or communicate with his professional colleagues. Thus, the effect of current classification procedures in this case may well be the opposite of what is intended. The Nation's security can be weakened rather than strengthened if bright engineers and scientists avoid working in defense-related fields or holding meetings on subjects which are close to defense interests.

In summary, I would like to make the following points:

One, an open communication system is an essential element in the operation of the U.S. engineering and science community.

Two, it is possible for industrially employed professionals to operate with both restricted and unrestricted information and still be active and effective participants in an essentially open communication system.

Three, that an open communication system is vulnerable to improper or careless application of classification procedures.

Four, those responsible for policymaking and policy implementation in classifying engineering and scientific information should be aware of the very substantial damage they can do to the U.S. technological enterprise.

Five, while decisions about specific situations will depend both on overall governmental policies as well as on judgments made by individual representatives of Federal agencies, wise decisionmaking will depend on having technically sophisticated people in the Federal agencies involved.

Sixth, it should be recognized that the United States must ultimately depend on the strength and accomplishments of its scientific and technical community for its national security. This community needs the freedom to communicate openly to retain its vitality.

Thank you for giving me an opportunity to testify, Mr. Chairman.

[The statement of Professor Willenbrock follows:]



IEEE

UNITED STATES ACTIVITIES BOARD

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.
1117 19TH STREET, N.W. WASHINGTON, DC 20036 U.S.A. TELEPHONE (202) 785-0017

TESTIMONY OF

DR. F. KARL WILLENBROCK⁴

CHAIRMAN OF THE IEEE TECHNOLOGY TRANSFER COMMITTEE

BEFORE THE

HOUSE JUDICIARY COMMITTEE

SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES

AND THE ADMINISTRATION OF JUSTICE

U.S. HOUSE OF REPRESENTATIVES

NOVEMBER 3, 1983

My name is F. Karl Willenbrock. I am Cecil H. Green Professor of Engineering at Southern Methodist University. I appear before you today as Chairman of the Technology Transfer Committee of the Institute of Electrical and Electronics Engineers (IEEE). This Institute was founded in 1884 and is a transnational technical society with more than 230,000 members worldwide. The Technology Transfer Committee which has developed this testimony is administered by the Institute's U.S. Activities Board, which is concerned with the public policy issues that affect the 190,000 Institute members who live in the United States.

The U.S. attained a position of world leadership in science and technology in the post World War II era. One reason for the success of the U.S. technological enterprise is that an extremely effective system of communication, among the professionals in the various disciplines, has been developed. At the heart of this communication system are the scientific and professional societies. I should like to give the Committee some indication of the scope and character of these societies by reference to the Institute of Electrical and Electronics Engineers, the leading professional society in the electrical, electronics, and computer fields. Almost all active fields of science and technology in the U.S. are served by one or more professional societies.

A major function of these societies is to provide the means for technical communication among the professionals in the various scientific and engineering fields and to create, for the future, a permanent record of the knowledge generated. The major modes of communication are the publication of journals and the sponsorship of meetings. At present, the IEEE publishes more than fifty technical periodicals (about 115,000 pages a year) and sponsors a minimum of 225 major technical meetings a year. In these periodicals and at these meetings, the theories, experimental results, and data that constitute the body of knowledge on which electrical, electronic, and computer engineering is based, are presented and debated. This procedure of research and discovery

followed by communicating the results to professional peers is an integral part of the process of the continuing growth of scientific understanding and the continuing development of new technological capability. The process engages participants ranging from the leading researchers in the field to the neophytes just entering the field. It stimulates new ideas and new contributions to knowledge and it disseminates this knowledge in a systematic and effective way to the professional community who will use it.

The vital role of the professional societies and the open communication systems they operate were brought home to me personally as the result of a trip I made to Indonesia last summer, I was part of a group from the National Academies of Science and Engineering whose objective was to advise the Indonesian Minister of Research and Technology on ways to make his country's scientific and technical programs more effective in that nation's development. It turned out that there are no effective professional societies in Indonesia and so the scientists and engineers there did not have available a systematic means of communication among the specialists in various technical fields. They had practically no knowledge of the programs and projects in the various governmental, university, and private-sector laboratories in their own country. It is not surprising that their rate of progress is slow. A slow rate of technological progress characterizes many societies in which free scientific and technical communication is inhibited.

In contrast, the U.S. has probably the most open system of technical communication in existence. The professional societies, as a major element in this system, continue to grow and expand their activities. Their resources are generated almost entirely from the dues paid by members and the sale of periodicals. For example, the 31 societies which constitute the IEEE represent the current specialties within the electrical/-electronics/computer community. As new fields of knowledge are created and new technologies emerge, additional societies or groupings will be formed within the Institute.

It is because these societies are so successful and contribute so directly to the advance of the various fields of engineering, science and technology that the science and technology community is greatly concerned with interference with their operations. Yet there have been an increasing number of occasions in which the dissemination of technological information has been adversely affected because of concern that information being disseminated would damage U.S. security. These occasions include the suppression of papers scheduled to be presented at conferences and modifications of papers submitted for publication.

It is of utmost importance for the continuing technological progress in the U.S. to examine the reasons for these interferences and to develop procedures to eliminate the conflict between the requirement of maintaining national security and the

necessity for free communications within the science and technology community. First, it should be understood that there are no procedural problems associated with information which has been clearly assigned a security classification by the appropriate governmental authority. Such information should not be published in unclassified periodicals or presented at open meetings. The IEEE editors and program chairmen have developed systematic procedures to avoid this possibility.

It is IEEE policy to require all authors to certify that the papers they submit for publication or presentation have been cleared by the appropriate authorities within their organizations.

However, difficulties arise when authors submit for publication or presentation information considered releaseable which is later declared classified or otherwise not publishable by a Federal agency representative. The actual clearance process through which these papers go varies considerably depending on the organization with which the author is affiliated. In industrial companies the usual practice is for all papers to be first cleared by company management to ensure that no proprietary nor classified information is being divulged. If there has been an external sponsor, such as the Department of Defense, clearance by a Federal program manager is usually also a part of the process. Since more than 60% of IEEE authors work for private companies, it is evident that these companies have developed techniques for their employees to actively participate in open

technical communication without harming the company's proprietary interests. University-based authors usually have a less formal clearance procedure depending on the sponsorship of their research. In any event, for all IEEE papers, the author is required to sign a statement at the time his paper is submitted to the IEEE that appropriate clearance has been obtained. Thus problems do not arise between the IEEE and authors. It is when a third party intervenes that problems arise.

It is noteworthy that the industry-based IEEE members operate with information, some of which is restricted because of its proprietary considerations and some of which is freely disseminated. These professionals contribute effectively to the open information system operated by the professional societies and yet do not damage their company's interests. If they did, companies would not continue their direct and indirect support of professional societies. The fact is that the leading U.S. technology-based companies encourage their employees' active participation in professional society publications, meetings, and other activities. It is evident that the dual objectives of protection of a company's commercial interests and the dissemination of new and state-of-the-art technical information are attainable. While the details of an industrial process may not be openly disseminated, the fundamentals of the process are usually open for public dissemination.

Incidents such as the widely publicized forced withdrawal of a large number of papers at the Society of Photo-Optical

Instrumentation Engineers (SPIE) Conference In the summer of 1982, the threatened forced withdrawal of papers at a number of IEEE conferences, and other such incidents, have led to difficulties between governmental and professional society representatives. In fundamental terms, the IEEE's relationship is with the author of a paper and through the author to the author's organization. When an external agency such as the Department of Defense asserts that some of the author's information should be restricted from open dissemination, the issue is really between the author and the agency, not with the IEEE. However to clarify what actually happens, I should like to describe a few incidents in detail and then seek to draw some general conclusions.

One such incident involves an article which was submitted by an external author for publication in the IEEE Spectrum last year. Spectrum is an award-winning monthly which is circulated worldwide to all IEEE members. Accompanying me today is Mr. Ellis Rubinstein, Managing Editor of Spectrum, who was directly involved in the incident. The article entitled, "Out-Numbered and Out-Weaponed by Soviets, the U.S. Army Shoots for High Technology," was subjected to the usual expert review process. Since the author quoted the Secretary of the Army, the article was sent to his office for review. A month and a half later, the Spectrum staff editors received a telephone call from the Army Office of the Chief of Public Affairs with the message that the manuscript contained classified information and should be shredded immediately. Upon questioning, the Army representative

identified three statements as being classified. The Spectrum staff investigated the origins of these three statements and found that two statements had been published in an unclassified widely disseminated Army publication entitled, "1982 Weapons Systems," and the third was from public testimony of the Army Chief of Staff to the 97th Congress. When this information was presented to the Army representative, it was agreed that the two published phrases were not really classified but that the Chief of Staff's testimony had been reclassified. The explanation was offered that sometimes unclassified information can be put together in such a way as to be reclassifiable. The issue was not pursued further since the article did not meet the technical standards appropriate for Spectrum.

However, the incident provides an opportunity to examine the effect that such actions can have on the scientific and technical publication community. Many authors of technical articles confronted with such a statement by a military representative would have withdrawn the article. In this case, a full-time editor of Spectrum who is not readily turned aside followed up and found that the reasons for withdrawal were at best questionable. The usual technical author -- who does not devote his full-time to paper-writing -- would tend to avoid topics that might be disapproved by a Federal agency, whether the information was classified or not.

Another incident occurred last year in connection with an IEEE-sponsored International Test Conference in Philadelphia.

Five days before the Conference was to open and after the conference publication had been printed, an official of Texas Instruments, Inc. requested, by telephone, that three papers written by TI engineers on Very Large Scale Integrated (VLSI) circuits be withdrawn because the U.S. Air Force Systems Command considered the release of these papers to be potentially damaging to U.S. interests. The authors, who are all IEEE members, had believed their papers were cleared having followed the usual procedures. Apparently the government reviewers did not decide until very late, that is until five days before the conference and after the Conference Digest had been printed and copies supplied to reporters, that the papers should not be published. The Conference managers were asked to excise the papers from the already printed Conference Digest and to ask reporters who had received pre-publication copies to return them. The Conference managers required that before taking these steps a written explanation of the reasons for removing the papers be given; that the authors themselves request removal; and that an agreement be made to pay the costs of destroying portions of the already printed record. In response to these requirements, a re-review of the papers by the Air Force resulted in a decision that the original papers could be presented as planned. Another incident occurred in 1982 in connection with the EASCON Conference held in Washington and sponsored by the IEEE Aerospace and Electronic Systems Society. Just before the Conference opened the chairman was asked by an Air Force representative to destroy all Conference

Records and to cancel the presentation of certain papers. The Conference chairman responded that he might agree to do so if the estimated cost of between \$25,000 to \$50,000 were borne by the Air Force. A day later, the Air Force representative withdrew his request. Later a Navy representative made a similar request which was also withdrawn after the costs were described.

In view of these incidents, it has become evident to the IEEE that it needed to develop a practical procedure to handle such cases. Typically the chairman of an IEEE technical Conferences program is an engineer employed by company or a university who undertakes this additional responsibility as a part-time voluntary professional society task. The IEEE is presently working on a "hot-line" procedure which will make available, to any Conference program manager or journal editor, access to the IEEE general manager's office so that previous experience with this type of situation is available. IEEE is also seeking to develop appropriate points of contact within DOD so that reasonable decisions can be reached in short periods of time.

The IEEE does not have a complete record of how many incidents of this type have occurred since they are not all reported to the IEEE General Manager. However there have been incidents in which papers have been withdrawn at the request of military representatives.

It is difficult, if not impossible, to measure the impact on the electrical/electronics community of incidents such as these.

Certainly they have a chilling effect on the science and technology community. I should like to cite two examples of such effects. One relates to an IEEE committee and the second relates to the research choices of an IEEE member who is a very capable junior engineering faculty member.

A number of IEEE members who are members of the Solid-State Circuits and Technology Committee canvassed their members to determine which topics would generate the most interest as focal points for proposed workshops in the Spring of 1982. Two topics selected were High Speed Technologies and the Very High Speed Integrated Circuits (VHSIC) program which the DOD has sponsored. Before going ahead with planning for a workshop on VHSIC, the DOD program manager's office was contacted. The manager's representative indicated that VHSIC was controlled by the International Traffic in Arms Regulations (ITAR). Therefore, if the workshop included information on chip fabrication and processes, chip architecture, internal details of the chip, and the performance details of chips, all workshop attendees would be required to present proof of U.S. citizenship. Such proof would not be required if only topics such as brass boards and the names of chips were to be covered. The IEEE group decided that those were too many constraints; the result was that the workshop was not held. Whether this decision was an advance, or a loss for U.S. national security is hard to decide. However, it is possible to assert that planners of this workshop, which included engineers

from Bell Laboratories, IBM, and the University of California at Berkeley, are among the most productive and capable engineers in the U.S. in this field.

A fellow faculty member at SMU, who recently completed his PhD at Princeton in communication theory, described to me several areas in which he felt very challenging technical problems existed. However, in his choice of topics on which to work, he has carefully avoided topics which are close to DOD interests because he feared his work might be classified. He considered this possibility disastrous because he would not be able to publish his results or communicate with his professional colleagues. Thus the effect of current classification procedures in this case may well be the opposite of the intended purpose. The nation's security can be weakened rather than strengthened if bright engineers and scientists avoid working in defense-related fields or holding meetings on subjects which are close to defense interests.

In summary, I should like to make the following points:

- 1) An open communication system is an essential element in the operation of the U.S. engineering and science community,
- 2) It is possible for industrially employed professionals to operate with both restricted and unrestricted information and still be active and effective participants in an open communication system,

- 3) An open communication system is vulnerable to improper or careless applications of classification procedures,
- 4) Those responsible for policy-making and policy-implementation in classifying engineering and scientific information should be aware of the very substantial damage they can do to the U.S. technological enterprise.
- 5) While decisions about specific situations will depend both on overall government policies as well as on judgments made by individual representatives of Federal agencies, wise decision-making will depend on having technically sophisticated people in the Federal agencies involved.
- 6) It should be recognized that the U.S. must ultimately depend on the strength and accomplishments of its scientific and technical community for its national security. This community needs the freedom to communicate openly to retain its vitality.

Thank you for giving me an opportunity to testify. If there are any questions, I shall be happy to respond.

11/2/83

Mr. KASTENMEIER. Thank you, Dr. Willenbrock, for such an excellent statement. It was a very useful statement.

Now we will hear from Professor Unger next, although I understand that Mr. Rubenstein could expand further on your testimony. Perhaps during the question and answer session we will have a need to refer to that.

The Chair would therefore like to call on Prof. Stephen H. Unger from Columbia University.

Professor UNGER. Mr. Chairman, I have also submitted a written statement and I will therefore not read it in detail. What I will do is elaborate on selected parts and make some comments that were stimulated in part by testimony of some of the preceding witnesses.

Mr. KASTENMEIER. Without objection, your statement will be received and made part of the record, and you may continue as you wish.

Professor UNGER. One of the focal points of my statement that I will come to toward the end will be a set of proposals for legislative action. It is my opinion that this situation calls for congressional action.

First I would like to say that the problem has frequently been falsely put in the form of a conflict between the personal rights and privileges of scientists and engineers and the national security. I submit that this is a false conflict in that there is no contradiction between these two interests.

As has been started by previous witnesses, the national security, to the extent that we define it in terms of military technology, is served by openness, not by secrecy. The same openness that enables scientists and engineers to exchange ideas freely with one another promotes the national security in the sense of enhancing the technological basis for that national security.

I would further submit—and in this case I agree with the chairman's earlier remarks—that national security should not be narrowly defined in terms of military technology or military power. There is a good deal more to it than that.

I would also argue that, given the strength of the U.S. military establishment, its enormous potential for retaliatory strikes, for example, with submarine-launched ballistic missiles, we are not in a situation where some marginal changes in technology would truly endanger the balance of power in the world. I don't see that at all. We are in a situation where the greatest danger is that unfortunate policies may precipitate a conflict that would destroy all concerned, not that we're going to be overwhelmed as a result of some technological advance made by the Soviet Union.

I shall skip over the discussion of why it is that the free exchange of information is vital to progress in science and technology, since I think this has been amply covered by previous speakers.

There is no doubt that a great deal of technology originating in the United States has been utilized by the Soviet Union to enhance its military strength. This is an inevitable consequence of the fact that the United States has originated most of the major technological advances in what is generally referred to as high technology. You cannot build a sophisticated missile system without using solid state technology that was originated in the United States. But any effort to shut off the flow of information in these fields would be

disastrous. You would literally have to restrict publication in this country to the extent that it is restricted in the Soviet Union.

Now, we may ask why it is that the Soviet Union is far behind the United States in advanced technology. It has been estimated, for example, that they are 5 to 10 years behind in the important fields of electronics and computers. This has been verified by an April 1982 CIA report, "The Soviet Acquisition of Western Technology". It is stated in that report the Soviet Union was about to go into full scale production of LSI, large scale integrated circuits. Now, this point was reached in the United States a full decade earlier. In 1972, to be specific, the Hewlett-Packard Corp. marketed a sophisticated, hand-held calculator based on LSI chips. So that by the admission of the CIA, the Soviet Union remains far behind us in this important field.

Note that for at least the past 5 years, the United States, Japan, and Western European countries have been producing VLSI [very large scale integrated] circuits, with roughly an order of magnitude greater density of components on a chip. The Soviet Union is not in the ballpark in this area.

Now, this is despite the fact that the Soviet Union has been graduating many more engineers and scientists than we have for probably a generation. The quality of the education given to these people is high. We know this because many emigres from the Soviet Union come to our universities and we find that they are competently trained.

There may be a number of explanations for their lag in high technology, despite this preponderance of numbers, but certainly most observers would agree that a major factor is the excessive secrecy endemic to that nation. It would seem to be a poor policy for us to abandon a winning strategy in favor of a losing strategy.

Now, apart from the issues that have been raised so far, I would like to introduce another consequence of secrecy in science and technology. This has to do with its effects on public policy. There are numerous issues, important issues, facing our country that have important technological aspects, that are, in fact, driven by technology issues. For example, should we fund the MX missile; what should be done about the acid rain problem; what about waste in Department of Defense procurement practices; arms control agreements (a complete nuclear test ban, a freeze in the testing of missile systems).

The ability to monitor arms control agreements with national means involves high technology. It involves the capability, for example, of our satellite observation stations. It involves the ability of seismographic instruments to detect underground tests. The problem of nuclear waste products—in fact, the whole area of nuclear energy—is highly technologically based. If we clamp down further on the flow of technological information, extending the realm of secrecy, we are going to make it impossible to have debates on these topics in line with our traditional American practices. There is no way in which we can properly resolve issues of this kind in the public arena if information is constrained.

For example, the current administration has issued statements indicating that we cannot reliably detect underground tests. Those statements were purportedly based on classified studies made under the aegis of the U.S. Government. Later the people who carried out those studies revealed that they had come to just the opposite conclusions.

Had we in force the kind of Official Secrets Act that exists in Britain, for example, these people could not have contradicted the misleading statements put out by Government officials. So I believe that from the political point of view, it is essential that openness in technology be maintained.

I have some cases illustrating Government imposed secrecy, but some of these were already covered and I think it's not necessary to hammer home that point further. Let me now present some ideas for handling this situation. First of all, I shall list some basic, guiding principles for legislation or other action:

One, secrecy should be restricted to specific details of direct military significance, details that would, if released, be helpful to an enemy or potential enemy in replicating or countering useful American military weapon systems. For example, it would be appropriate to classify the details of specific decoys to be used with ICBM's of some class; that is, the detailed characteristics that would be useful if somebody were trying to get around those decoys. It would not be appropriate to classify the concept that decoys are going to be used, because you can't conceal that sort of thing anyway and it is necessary in debating the efficacy of defense systems and of attack systems to have that kind of information in the public realm. A proper discussion of the feasibility of using satellite-based lasers to destroy missiles is impossible without a fairly good general understanding of the kinds of tactics that can be used to counter such a system. Therefore, secrecy should be confined to the most detailed points.

Let me digress for a moment to show why it would not be damaging to release general information relevant to weapons systems. An important point that has not been discussed is how technology transfer is actually carried out. There exists extensive experience in the process of transferring technology to people in other countries or even in other companies within our own country. This is not accomplished by merely turning over pieces of paper. If a company in this country wants to sell an integrated circuits plant, let's say, to an organization in Italy, they send over experts with the hardware to show the employees of that other company, in detail, how to use that equipment.

Furthermore, they may invite people from the other country to come here and participate in production processes. The kinds of details that allow people actually to implement technology on a day-to-day basis must be conveyed in a very personal manner, not just by handing over pieces of paper. We have a lot of experience to indicate that that is not adequate. Thus published information is not nearly as important in conveying know-how as is suggested by proponents of secrecy.

To continue with the basic principles, the need for secrecy should be balanced in each case against the value of releasing the infor-

mation. One should not assume that just because there is some argument for secrecy that we should impose it.

The burden of proof should be on the advocate of secrecy.

In each instance where an item is declared secret, it should be declared secret for some specified time interval. After that time interval it should either be released or the case for secrecy should be remade.

There should be an appeal procedure, independent of the agency doing the classifying, and there should be a documentary record to facilitate accountability for making things secret, so as to discourage casual acts of censorship.

Mechanisms should be established to deter the overzealous use of secrecy; that is, there should be some penalty against those who overclassify. There are natural tendencies to overclassify. One who has the ability to make something a secret will always have the feeling that the safe thing to do is to declare it secret. For one thing, "if you declare it secret, you can always release it later" is the argument; whereas, once you let the cat out of the bag, then that's the end of it. Furthermore, people can easily be criticized for releasing something, but if they don't release it, nobody knows what it's all about so they can't be criticized. Therefore, to balance this, we need some mechanisms for deterring the overzealous classifiers.

Provision should be made for congressional oversight of secrecy regulations.

No attempt should be made to restrict basic scientific and engineering knowledge or information that is important in assessing the efficacy or cost of a military system.

Now, it would be very nice if those in the executive branch of Government would, of their own accord comply with the principles outlined above. But, unfortunately, we have some 40 years of history, spanning administrations of both parties, to indicate that this is not likely to occur. This is not something endemic to one political party. Those who have the power to use secrecy are going to use it, and they are going to abuse it. We know that.

For example, around 1970 there was a report by a Government-appointed committee (chaired by Frederick Seitz and including Edward Teller) investigating the extent of classified information in the United States. It was found that something like 90 percent of the scientific and technical information classified should not have been classified. The conclusions were ignored and the report itself was classified.

Therefore, I believe that negotiating with members of the executive branch is not the answer. Congress must act—in two ways. One is that it should be clearly stated in law that the various regulations, such as ITAR, the Commerce Department regulations, the Invention Secrets Act, the Export Administration Act, et cetera, should be interpreted as not to permit restrictions on information that is not classified. I would make that a blanket, overall statement, not leaving any gray areas for officials to exploit. Our experience is, if you leave a loophole, they will drive elephants through that loophole. It is fine to say we can identify very narrow gray areas, but in practice I don't think that can be done.

Therefore, I would force the Defense Department or the administration in general explicitly to classify material that they feel is of national security importance.

We would then have to do something to ensure that this area of restriction not be made unduly large, that is, that they just don't go around classifying everything. Over the years, the system of classification has grown by virtue of a series of Executive orders issued by various Presidents of the United States. There is nothing in the Constitution authorizing the Executive to issue what amounts to legislation. This encroachment has been permitted to continue by default. I feel that in this particular area the abuses are so great and the danger to the country is so great that the Congress should step in now and reassert its power to legislate and take away that power from the executive branch.

So I would propose that a specific piece of legislation be passed which could be considered either as constraining Executive orders in this area, or replacing such orders.

With regard to classified information, the law should require that: specific harm anticipated by release of the proposed classified material be described in detail; the specific harm considered if the information is not released should be described; a case be made for the proposition that more harm is likely to result from the release than from the suppression; doubtful cases be resolved in favor of openness; the proposal for classification include a time limit, as indicated earlier; classification be applied to specific pieces of information, not to entire documents that may also deal with matters that don't merit classification; there be an appeal procedure outside the agency and that this appeal procedure be subject to congressional oversight—and I would suggest one way to do this would be for a congressional committee periodically to survey randomly-selected cases, examine the documentation, and determine whether proper action was taken; those found responsible for repeatedly overclassifying information by this process should be deprived of classification authority.

Now, if this were done, I believe it would greatly reduce the amount of classified information and would play an important role in freeing us from these problems.

In conclusion, I would like to say that we have here a situation where the freedom that we talk about, that we cherish so greatly in this country, is being underestimated. It is not being resorted to as a source of strength. The concept of openness, both in society in general and in the realm of science and technology—and the same reasons motivate both—is not a fragile luxury to be enjoyed only in tranquil times and abandoned when the going gets rough. On the contrary, it is a robust mechanism for coping with difficult matters, and its value is greatest in situations of maximum stress. It would indeed be tragic if a loss of nerve, brought about perhaps by a distorted view of reality, should cause our country to abandon what has been one of its principal sources of strength.

Thank you, Mr. Chairman.

[The statement of Professor Unger follows:]

Government Imposed Secrecy in Science

For the Committee on the Judiciary, US House of Representatives

Stephen H. Unger

Computer Science Department

Columbia University

New York, New York 10027

1 November 1983

1. Introduction

1.1. A Pseudo-conflict

It has been argued (e.g. by Admiral Inman) that the question of determining the extent to which scientific and engineering knowledge should be kept secret must be determined by balancing the rights of scientists and engineers against the needs of national security. This formulation of the problem is seriously misleading. There is actually no significant conflict between national security and the rights of those who develop and apply scientific and engineering ideas. On the contrary, *both* of these interests are best served by the openness that characterizes basic American traditions and the scientific process. Secrecy, with few exceptions, undermines the national security by impeding progress in the development of the technology which is one of its important pillars.

The free exchange of knowledge among scientists and engineers is a key factor in promoting progress. An integral part of the scientific process is the publication and wide dissemination of new ideas, discoveries, and experimental results. By this means, critics may detect errors or faulty reasoning, point out possible improvements, or confirm the validity of what was done. Colleagues (often complete strangers) may suggest solutions or alternative approaches to problems raised. They may find applications other than those that the author had in mind—sometimes in entirely different fields. Mention in a technical paper of unsuccessful approaches to a problem helps others avoid wasting effort in exploring blind alleys. Publication of successful solutions to problems makes it unnecessary for others to expend time and energy in solving them again, although it is common for a solution to inspire others to find better, often simpler, solutions to the same problems. They may also generalize the published solutions to cover a broader class of problems.

Both those who publish results and those who read about them profit. Science is a vast co-operative enterprise in which the free communication of ideas is a crucial element. The wider the community to which ideas are exposed, the more effective is the process. One may also use the analogy of a free market of ideas in which the good ones tend to prosper and the defective ones are discarded (or mended).

But why should we permit the fruits of American research and development efforts to be used to improve the quality of the Soviet military establishment? Don't they benefit greatly by using technology originated by us? Wouldn't we be more likely to retain our technological superiority in weaponry if we curtailed the dissemination of information in areas of technology most relevant to military systems?

First, there is no doubt that a great deal of technology originating in the USA has been utilized for military purposes by the Soviet Union. This follows from the fact that we have been in the forefront of scientific and engineering progress since World War II, particularly in the related areas of electronics and computers. It is not possible to build any advanced military system without utilizing concepts developed by Americans.

It therefore follows that, if we could somehow shut off, or even significantly attenuate, the flow of technological knowledge between the USA and the USSR, weapons (as well as general industrial) development in the USSR would be slowed. But this does not necessarily mean that we would thereby increase our lead in technology. There is no way to block the flow of information to the Soviets without *also* seriously restricting the flow of information within the American technological community. The probable result would be that the damage at home to the scientific process outlined above would slow our own progress more than it would slow theirs. A significant factor here is that a large portion of material published in the journals of the technological leaders is on topics that are of little interest to those lagging behind, simply because the latter haven't yet reached the point where they could utilize the results

discussed. Another secondary harm that would result is that when certain topics are judged to be of sufficient importance to the national security as to justify being subjected to censorship, those researchers in this country who have the freedom to choose the problems that they work on would tend to avoid those areas so as to escape the onerous burden of operating under a veil of secrecy. A rather different consideration is that the USA by no means has a monopoly on high technology. Unless Japan, Canada and most West European nations followed the same restrictive policies, their effect would be severely limited. Efforts to pressure them into doing so, or to include *them* in the forbidden area could have serious detrimental effects on our international relations.

2. Is There Really Cause for Alarm

Despite the fact that there have been no governmental efforts (until recently) to impede the publication of ideas in computers and electronics, the Soviet Union has lagged far behind in these fields, and there is little evidence that they are making significant progress in closing the gap. Interesting support for this assertion is contained in a 1982 CIA report, "The Soviet Acquisition of Western Technology". It mentions that the Soviet Union was, at that time, beginning to get into full scale production of LSI (large scale integrated) circuits. Fully ten years previously, Hewlett Packard began marketing sophisticated hand-held calculators utilizing LSI technology. The US, Japan, and several West European nations have, for at least 8 years, been commercially producing chips containing many times the number of active elements incorporated in LSI chips; I refer here to VLSI (very large scale integration) technology. It is clear from this same report that, from a practical point of view, the most advanced Soviet use of Western ideas in electronics is in the form of imported equipment used in the production of integrated circuits.

Why are the Soviets so far behind, despite the fact that their educational system has, for a generation, been producing many more scientists and engineers than has ours? It is not because that system is of low quality; on the contrary, scientists and engineers who have emigrated here from the Soviet Union, including recent graduates and students, appear to be reasonably well educated by American standards. A factor generally accepted as an important part of the explanation (though by no means the complete explanation) is the deeply rooted and pervasive practice of secrecy. Within the Soviet Union a compulsive concern with secrecy has severely hampered the cooperative aspect of the scientific endeavor.

There is little reason to believe that the Soviets are threatening our lead in high technology, and ample reason to have confidence that openness is likely to continue to prevail over secrecy.

3. Science, Secrecy and Public Policy

It has been argued above that impeding the flow of technological knowledge is a counterproductive approach to a non-existent problem. If the public policy implications of secrecy are examined, it becomes evident, that the damage wrought to the day-to-day working of the scientific process is reflected on another level by similar damage to the democratic decision-making process.

A great many issues of national importance involve significant technological aspects. If information about the technology involved is made secret, then a meaningful debate becomes impossible, and those who control the flow of information can dominate the decision-making process. Their decisions will be made without benefit of the same sort of critical exchanges that were described above in connection with the scientific process. There is ample historical evidence that a closed decision-making process is prone to all manner of dangerous blunders. It is of course a basic premise of our own system that an open, democratic process is the best way we know for minimizing harmful error.

Should the present trend to clamp down on the flow of technological information continue, consider the

effects on debates involving such critical matters as:

- The MX missile
- Acid rain
- Waste in DOD procurement practices
- The use of Satellite based lasers for defense against ICBM's
- The ability to monitor arms control agreements

It is clearly central to the concept of government envisioned by the authors of the First Amendment that the information necessary for intelligent discussion of issues such as these be freely available.

4. Some Illustrative Cases

Reference has been made to governmental efforts over the last several years to enlarge the realm of secrecy to encompass information developed outside of the areas usually regarded as subject to secrecy, i.e. DOD facilities or classified projects undertaken by DOD contractors. Only a few examples will be presented here; it is assumed that others will present additional cases, or that reference can be made to other sources, such as my article, "The Growing Threat of Government Secrecy", in the February/March 1982 issue of Technology Review.

In 1980 the Rohm and Haas Chemical Corporation filed a patent application for an improved storage battery that they had developed in their own laboratories with company funds. The response from the Patent Office was a secrecy order, issued at the request of the US Army under the authority of the Invention Secrets Act. It took the company about six months to get the order rescinded, during which time all work on the battery was halted.

In 1982, 3 papers based on work done at the Texas Instruments Corporation under an unclassified Air Force contract were submitted for presentation at an IEEE (Institute of Electrical and Electronics Engineers) conference on reliability were the subject of a furor over secrecy. Although the papers were on an unclassified subject, dealt with no military related matters, and had been approved for publication by the contract monitors, a different set of Air Force officials decided about a week before the conference (and after the conference proceedings including the 3 papers had already been printed) that the papers should not have been cleared. Strenuous last minute arguments led to a withdrawal of the objections to presentation.

Perhaps one of the more absurd episodes occurred in 1976, when the distinguished Soviet physicist L. I. Rudakov delivered a series of lectures at a number of American research laboratories on his work in electron-beam fusion. One can only speculate as to why ERDA officials chose to notify those at each host laboratory that the subject matter of Rudakov's lectures was classified so that the ideas he presented should not be disseminated.

5. Proposed Remedies

5.1. Basic Principles

I suggest that the following basic principles be used as guides in formulating solutions to the problems discussed above:

1. Secrecy should be restricted to specific details of direct military significance that would, if released, be helpful to a potential enemy in replicating or countering a useful American military weapon or system. e.g. It would be appropriate to classify the details of specific decoys to be associated with some class of ICBM's.
2. The need for secrecy should be balanced in each case against the value of releasing the information.
3. The burden of proof should be on the advocate of secrecy in each case.
4. In each instance where an item is declared secret, a time interval should be specified after which the case for secrecy must be made again, or the item must be released.
5. There should be an appeal procedure, independent of the agency doing the classifying.
6. In order to facilitate accountability, and to discourage casual acts of censorship, written records should be kept justifying the case for secrecy in each instance.
7. Mechanisms should be established to deter the overzealous use of secrecy.
8. Provision should be made for congressional oversight of secrecy regulations.
9. No attempt should be made to restrict basic scientific and engineering knowledge or information important in assessing the efficacy or cost of a military system.

It would be a happy situation if those in the executive branch of government acted in a manner consistent with the above principles. Unfortunately, more than 40 years of history makes all too clear the fact that both military and civil administrators are unable to resist abusing the power to withhold information. (The disappointing lack of a positive response by the present administration to the very conciliatory approach taken by the Corson Committee serves to underscore this point

There is thus a pressing need for legislation to reverse the trend that, if left unchecked, threatens to

stifle our scientific and engineering efforts under a veil of secrecy. What follows are two specific proposals aimed at restoring a balanced view of the role of secrecy in promoting the national security. The first deals with regulations such as the ITAR that derive from existing legislation, and the second concerns regulations derived from executive orders.

5.2. Clarifying Existing Laws

A few years ago, DOD official Larry Sumney said that "the ITAR, if enforced to the letter would cover virtually everything done in the United States." (He was referring to a combination of clauses and footnotes that, in combination, would require prior government clearance for publication of material on any topic that was remotely relevant to a wide range of military applications. In the 1977 IEEE cryptology episode, an attempt was made to use just such provisions of the ITAR to coerce the IEEE into cancelling the presentation of certain papers.) Although Sumney added that they have never been so applied, the fact remains that such regulations depending on the good sense of bureaucrats to avoid serious abuses have no place in our system. Even if not actually enforced, they may cause people to refrain from communicating information out of fear that some official may suddenly decide to apply them strictly.

It would clear the air if Congress were to pass a law that would clearly state that no provisions of the Arms Control Export Act, the Export Administration Act, the Invention Secrecy Act, The Atomic Energy Act, or any other legislation should be interpreted as authorizing restrictions on the dissemination of scientific or engineering information not derived from classified projects. In particular, the "born secret" concept should be stricken from all laws and regulations. (Rather than passing a single law, it may be necessary or desirable to amend each existing relevant piece of legislation to attain the same end.)

The result of such action would be to prevent further attempts by government officials to interfere with the dissemination of knowledge generated by people working outside of areas clearly marked as classified for security reasons. Next it is necessary to ensure that this restricted area not be made unduly large.

5.3. Controlling the Classifiers

The system under which information is declared classified grew up in a rather haphazard manner over a period spanning the administrations of perhaps nine presidents. Congress played essentially no role in its development. Now that it is evident that this system has profound effects on our nation's course as well as on the lives of its citizens, it would be highly appropriate for the Congress to remedy what is evidently an encroachment by the executive branch on its lawmaking powers as spelled out in the constitution. I propose that legislation be enacted either to replace or to restrict executive orders pertaining to the classification of information. (I am addressing myself specifically to scientific and engineering information, although it may be desirable to cover the subject more broadly at one stroke). In conformity with the aforementioned list of basic principles, the following points should be incorporated in any procedures for classifying scientific or engineering information:

1. Specific harm anticipated by release of the information to be classified must be described.
2. Specific harm considered if the information is not released must be described.
3. A case must be made for the proposition that more harm is likely to result from the release of the information than from its suppression.
4. Doubtful cases must be resolved in favor of openness.

5. The proposal for classification must include a time limit after which the information must be released or the case made anew.
6. Classification must be applied to specific pieces of information- not to entire documents that may also deal with matters that do not merit classification.
7. An appeal procedure should be set up *outside* the agency doing the classifying, for *timely* hearings of complaints about improper decisions to classify information.
8. The workings of the appeal process should be subjected to congressional oversight by means of periodic reviews by a congressional committee of randomly selected cases. To facilitate this accountability process, each application of the procedures outlined above should be fully documented.
9. Those found responsible for repeatedly overclassifying information should be deprived of classification authority.

It should be evident that, if the above ideas are implemented, classifying technical information would entail considerable thought and effort. It would be done only where significant matters were involved, and abuses would be much easier to detect and correct. The result would be a great reduction in the amount of classified information. This is precisely what is intended.

6. Conclusions

The proposals made here depend on the premise that the harm done by secrecy is of a far reaching and pervasive nature, and that it significantly outweighs the damage that might be wrought by an occasional instance where a particular piece of information proves to be of value to a real or potential enemy. No doubt one could cite real or hypothetical instances where the suggested procedures would fail to protect some piece of information to the detriment of the nation's security. But it must be understood that human institutions are inherently imperfect; no system can be expected to operate flawlessly. In particular, any system that attempts to prevent all instances in which useful information passes across an unfriendly border will inevitably wreak havoc within our own borders that will be far greater than the damage that it seeks to avoid.

The concept of openness both in society in general and in the realm of science and technology is not a fragile luxury to be enjoyed in tranquil times and abandoned when the going gets rough. On the contrary, it is a robust mechanism for coping with difficult matters, and its value is greatest in situations of maximum stress. It would indeed be tragic if a loss of nerve brought about perhaps by a distorted view of reality should cause our country to abandon what has been one of its principal sources of strength.

Mr. KASTENMEIER. Thank you, Dr. Unger, for that very helpful presentation. It was very precise in terms of recommendations on how we might improve the situation.

I take it there are some respects in which your testimony agrees with other witnesses, particularly the two that appeared before the panel of which you're a member, and other respects in which it does not. You do not quite share the concern about the dangers of technology transfer to others, including the Russians, that I guess particularly Dr. Press speaks eloquently to.

Is that right? Do you feel there is less loss because of that than is made out, that the other values that are harmed in the process, our own ability to proceed with untrammelled scientific inquiry, is compromised thereby?

Professor UNGER. I agree with the conclusions of the Corson panel, that whatever harm is done by the transfer of technology is done through the transfer of hardware, of equipment, rather than pieces of paper. So I do agree with that.

However, it is my impression that the Corson Committee's recommendations were in the nature of a compromise, that they were attempting to accommodate views that they didn't necessarily agree with. Now their position is being regarded as an extreme position from which compromises are to be made. I believe this is very unfortunate.

Any attempt to shut off the flow of information to the point where no harmful information will get through will inevitably fail, or it will be so stringent that it will destroy our country in the process. In other words, we would have to become very much like the Soviet Union in order really to shutoff that flow. We have to recognize that any reasonable system that we set up will occasionally allow some pieces of information of real value to get through; we have to accept that as a cost in the real world of doing business.

Mr. KASTENMEIER. Thank you.

Dr. Willenbrock, I notice that you and Professor Davida in your testimony both suggested, at least indirectly, that requests of the Federal Government—whether these are agents of the Air Force or Department of Defense or whatever—were at best either arbitrary or capricious. They say that because in Professor Davida's case they later, when you resisted, withdrew the order.

Professor DAVIDA. Yes, they did.

Mr. KASTENMEIER. And in the case of those who resisted either in terms of the restrictions on meetings or otherwise, placed conditions on them with respect to your compliance, they then withdrew their request or their insistence on destroying certain publications, which would suggest that the urgent underlying interests of national security were not that great in any of these particular matters.

Do you have any comment?

Professor WILLENBROCK. Yes. Those incidents are some of the cases we were able to document, Mr. Chairman. These are events as they occurred. One can certainly draw the conclusion that there is an overzealousness to classify and that quite frequently, when subject to further investigation, it turns out not to be as significant as originally thought. That is why I made reference to the industrial community where they seem to have worked out some of these

problems. Engineers operate with some restricted information, some unrestricted information, and they don't shoot themselves in the foot in the process.

There can be cases where classification is necessary; no one is arguing about that. But the incidents involving the late application of classification and also the reclassification of already published material don't make much sense.

Mr. KASTENMEIER. But on the other hand there is some effect, even the withdrawal of these requests, or whatever the nature of the entreaty to you was. You indicated there was at least one other conference that was canceled rather than——

Professor WILLENBROCK. There are cases where papers were actually withdrawn. In one particular case the program manager just withdrew them. He felt that's all there was to it.

Actually, in response to a question asked of the previous testifiers about 2 years ago the Institute set up a technology transfer committee just to monitor, keep track of, and be concerned about such issues, and to try to develop appropriate procedures. We know how to run conferences. But a new constraint is being laid on the program managers, to learn how to handle these situations which frequently come up at the last minute. Trying to get a good system inside the Institute is what we're working on right now.

Mr. KASTENMEIER. I guess the point I was making was, even though you may have succeeded in thwarting some intrusions into your conferences and the like, there is a chilling effect that remains nonetheless. Anyone planning a conference hereinafter, or the publication of technical papers, has to wonder whether they really want to go through with it or not and subject themselves to this sort of supervision by governmental officials and any objections that may lie—and, indeed, whether they violate some law in connection with it which would subject them to severe penalties.

Professor WILLENBROCK. That's exactly the point, Mr. Chairman. That's exactly why we feel the present situation is not a desirable one. We are trying to learn how to operate with it, but we certainly would hope that the Congress could undertake to help get the situation clarified so that we don't have these very ambiguous situations.

The penalties involved in the ITAR's and the EAR's are very severe. It is not as if they can be just ignored. You really can scare people—and people really are scared—because of these sorts of events. People read about them and the impact is a significant one.

Mr. KASTENMEIER. Professor Unger?

Professor UNGER. I would like to illustrate the point that you just made in connection with one of the examples that Dr. Willenbrock gave, namely, the attempt to withdraw those three papers from the IEEE Reliability Conference, the ones from Texas Instruments, which was reversed after the furor was raised.

In the reporting of that incident, it was indicated I believe by the vice president of Texas Instruments who at the end said "We're not going to get into this kind of situation—" and I'm not quoting him directly, of course—"We're not going to get into this kind of situation again. We're going to be very careful in the future before we permit such papers to be published."

I might mention that I have seen those three papers. They're in an area that I'm familiar with. They had absolutely nothing to do with any military application. They were papers of exactly the kind that are published all the time in IEEE publications.

Mr. KASTENMEIER. On a different subject—and I'm just giving this for the record—in fiscal years 1980-83, in terms of patent secrecy orders issued, there were 1,306. In 1980, 279; in 1981, about 253. But 1982 went up to 350, and already in 1983 it is 424. I was interested in whether there was some trend toward—maybe one can blame it on technology, or one can also wonder whether it's overzealousness with reference to protection in that regard.

Ironically, perhaps, this subcommittee, in addition to civil liberties—which is really the overall subject of this hearing is, as I think you now, in charge of legislation in the area of copyright and patents. One of the issues before us in terms of computer systems is what, if any, sort of protection should be afforded the semiconductor chip in terms of commercial protection as a proprietary interest in the design or whatever is imbedded in the chip, which is quite a separate question, but nonetheless is, in terms of technology transfer and other questions, not wholly unrelated. But we are interested in what is happening and whether or not there is an increasing pervasive presence of inhibiting governmental restrictions with respect to science and technology and to what extent it is justified.

Finding a balance is very difficult because if there is either an overriding or at least an important national security justification, as with the other two witnesses, it is very difficult to determine that. It is extremely elusive, it's highly subjective, actually, unfortunately. It depends on one's fears, what one anticipates, and it even has a base in ideology which makes it unsusceptible to easy legislative resolution. But I do admire the principles and the suggestions made by Professor Unger with respect to secrecy.

We have a vote on and I'm going to have to leave. I think this will conclude the hearing today. I hope that we can rely on perhaps occasion to impose upon you again, either by correspondence or otherwise, for your wisdom and your contributions, your experience in these fields, particularly in this area, which I think needs to at least be elevated in terms of public perception or visibility as a major public policy question for us to resolve.

Accordingly, I thank you for your contribution. This concludes the hearing today and the committee is adjourned.

[Whereupon, at 1:07 p.m., the subcommittee was adjourned.]

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

TUESDAY, JANUARY 24, 1984

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 9:30 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Schroeder, Frank, DeWine, Kindness, and Sawyer.

Staff present: David W. Beier, Deborah Leavy, counsel; Joseph V. Wolfe, associate counsel; and Audrey Marcus, clerk.

Mr. KASTENMEIER. This morning, the subcommittee continues with a third day of hearings on 1984: Civil Liberties and the National Security State.

During the first 2 days of hearings, the subcommittee focused on various attempts by the executive branch, this administration and its predecessors, to restrict the free flow of information.

Today's hearing inquires into another area for civil liberties concern: Aspects of individual or personal privacy in an era of dramatic changes in technology.

The basic theme of our hearing today is to evaluate the adequacy of our laws regulating the interception of electronic communications. Other subcommittees of the Congress are investigating the question of computer crime.

What has been missing from that debate is a moral or philosophic understanding of the interests which are protected by laws against the interception of communications.

In this regard, we can perhaps benefit from examining the history of privacy protections for private communications.

In early colonial times, private communications were primarily carried on through the use of private mail systems. Despite admonitions by some Government officials not to open the mail, such openings were such a frequent practice that Thomas Jefferson and George Washington both feared to write what they thought.

Eventually, the protection of the mails was achieved through a combination of laws and a dramatic increase in the number of messages delivered. The more messages sent, the more difficult it became to identify which letter to intercept.

In the 19th century, the new technology was the telegraph. One of the major privacy issues that occupied Congress in the 1870's was whether the records of Western Union should be opened up for random searches by congressional committees. Much of the debate focused on whether the parties using the telegraph had a reasonable expectation of confidentiality.

Finally, in the 20th century, new methods of communications were developed such as the telephone, computers and other forms of electronic communication. Initially, the courts and the Congress were reluctant to proscribe interception of such communications. Eventually, the wisdom of Justice Brandeis was accepted with respect to voice communications.

Brandeis said: "Every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the fourth amendment."

One of the issues we will take cognizance of today is the failure of title III of the Omnibus Crime Control and Safe Streets Act of 1968, the so-called wiretapping statute, to proscribe the interception of communication that is transmitted in nonvoice form.

Before we address the narrow technical question, however, we are well-advised to stress the values that are preserved by free and open communication.

Each of us as autonomous human beings has an inalienable right to think and communicate without unwarranted intrusions. Protection of these rights is the essence of personal privacy. Our task today is to begin an inquiry into the adequacy of those protections.

At first, I would like to start by greeting and calling up a panel consisting of three leading specialists in the field of electronic surveillance. Each of the gentlemen brings a slightly different perspective to evaluating the sufficiency of our current wiretapping statutes.

Professor Schwartz is an old friend who served as a civil libertarian influence inside and outside the Government.

Professor Schwartz will focus on the interplay between electronic surveillance and national security concerns.

Prof. Michael Goldsmith of Vanderbilt University, he is currently on leave, and with the New York State Organized Crime Task Force, an author of a recent seminal article on wiretapping.

The final member of the panel is Magistrate James Carr. Magistrate Carr is the author of the leading text on the subject at hand, electronic surveillance.

Gentlemen, would you come forward? We have received your written statements, and so, if you care to proceed either from your written statements or as you wish, your written statements will be made part of the record.

TESTIMONY OF HERMAN SCHWARTZ, PROFESSOR OF LAW, AMERICAN UNIVERSITY; MICHAEL GOLDSMITH, ASSISTANT PROFESSOR OF LAW, VANDERBILT LAW SCHOOL; AND JAMES CARR, U.S. MAGISTRATE

Mr. SCHWARTZ. It is always a pleasure to appear before your subcommittee. One always has the feeling that in this subcommittee

the flame of concern for civil liberties, no matter how bad the times, burns very brightly indeed.

I would like to comment on the national security issue growing out of the very important hearings that this subcommittee held a few months ago, as well as on some other topics of current interest, and I hope I won't range too far afield from the topics that you laid out as the current concern of the subcommittee.

I have a statement which I have submitted, and I will try to sort of read through it without reading it that precisely.

The issue of national security is a very vexing one, obviously. It has always been so powerful a notion that as Egil Krogh noted a few years ago, merely invoking it is enough to virtually silence all discussion and criticism, and it is, therefore, particularly important that hearings like these be held so that we may try to impose some legal controls, democratic controls, over a practice like electronic surveillance, which does indeed lend itself to abuse so easily.

And I want to commend you for holding these hearings and for having the determination and courage to do so, because it probably takes both.

I will talk about the Foreign Intelligence Surveillance Act. I don't have too much more to say that I didn't say in an article that I published some months ago following the hearings of this committee, except to respond to some of the comments made by the Attorney General in response to questions put by the committee.

As we all know, the evil at which the FISA Act was aimed in 1978 was the indiscriminate targetting of Americans for purposes wholly unconnected with national security, for political or personal security.

I did a pamphlet for the Field Foundation in 1977, and I tried to pull together some of these examples which go back to the Roosevelt administration in the thirties, and I would like to attach as part of my testimony some of the pages from that pamphlet.

Mr. KASTENMEIER. Without objection.

Mr. SCHWARTZ. Thank you.

I guess the question is how well has this statute which has been in effect since 1979 worked, and the answer is, we don't know. I tried to pull something out of the hearings, but for obvious reasons many of the witnesses did not say much.

I would also like, if I may, to include that article as part of my testimony.

I raised four troubling problems. During the 19 months of the Carter administration, it used the FISA statute some 529 times. It is hard to know how many taps and bugs were actually installed in those years, because some were extensions.

In the first 2 years of the Reagan administration, the number of surveillance orders granted by the judges rose to 433 in 1981 and 475, respectively.

Why? Were the additional taps and bugs used to eavesdrop on Americans? Second, the judges have not denied a single Government application. Does that mean the court is a rubber stamp? Maybe it is because the applications are so good, but I have seen some others that were not so good that were approved.

The reports of intelligence taps have surfaced in criminal cases. That is nothing new. Yet, the courts have done almost nothing to

ensure that the looser standards of the FISA statute, which have no notice provisions, for example, and are looser than are required for title III criminal prosecutions, there is no assurance FISA is not being used for law enforcement purposes.

I would like to refer to my article with respect to each of those, and if you have questions, I will be happy to answer them.

I should also like to discuss some of the answers that the Attorney General provided the subcommittee. First, with respect to the annual reports by the House and Senate Intelligence Committees, I believe they should be continued.

If ever there was an area where eternal vigilance is the price of liberty, this is it. I don't have enough confidence in the Judiciary, particularly where matters of national security are concerned.

I think that is demonstrated to some extent by the alacrity with which the special FISA court granted warrants for physical searches which are clearly not covered by the statutes.

The reports don't tell us too much, but they offer an opportunity for reflection and review about these questions and they ought to be continued.

With respect to the Attorney General's response about the interplay between title III and FISA, I can only say that this is a terribly difficult problem that has simply not been properly met.

As I indicated in the article, it is hard to see the Government ever losing this issue, given the fact that the issue is decided ex parte and in camera. Yet the prospects for abuse are very substantial.

It is difficult for me to see why, if the purpose of FISA is solely to gather intelligence, the use of FISA-obtained information should not be restricted to that.

Although the statute may indeed allow use of FISA-obtained intelligence in criminal proceedings, an effort should be made to limit this to situations where the Government can overcome a presumption that where the FISA surveillance is conducted at or near the time of indictment, the purpose of the surveillance was for the prosecution.

This, of course, does adopt the primary purpose test, but tries to make it a little more realistic in operation.

Incidentally, if a title III intercept is installed, continuation of this FISA surveillance for the purpose of gathering intelligence would rarely seem necessary since the title III interception would usually produce the same kind of information.

As to public divulgence of the number of targeted "U.S. persons," the claim that this "might allow some foreign powers to estimate the percentage of their clandestine agents who are known to the U.S. Government and are under surveillance and, conversely, the number we are not aware of" may well be valid.

I must say, however, that this is such a boilerplate stock response by the Department of Justice and the intelligence agencies to any request for information that it is hard to take at face value.

Two years I requested a breakdown of title III taps for fiscal year 1982 by offense. I was forced to file an FOIA suit to get this data because the Department's initial response was that making this data public "would aid persons in committing certain categories of offenses by informing them of the probability of whether they will

be, or have been, subject to electronic surveillance pursuant to title III" even though the very same information is provided to the public every year on a calendar basis.

As soon as the suit was filed, the Department promptly turned over the data, with apparently little concern for the jump in the crime rate they had earlier feared so much.

Let me note finally that the Department's response to the committee's concern about interception of attorney-client communications, that the "use" of such interceptions is limited, obviously evades the issue.

For one thing, use and limit are ambiguous; also, the effort to monitor whether such limitations are indeed imposed will often be futile.

This so-called limitation on use is consistent with the Department's past history of listening in on such conversations. The rule ought to be that whenever it becomes apparent that the conversation is between an attorney and his or her client, the interception should be turned off until the conversation is over.

That is all I have to say about the national security problem. These are not terribly profound remarks, primarily because we don't know very much about how FISA is operating. The interest of this subcommittee in the matter is thus terribly important.

Let me turn to the consent taping problem. There really is no excuse or justification for the taping by Mr. Wick. The New York Times and the Washington Post reported this morning that the GSA had established that it was a violation of GSA and Archives rules about destruction of the transcript.

It is really very easy to amend title III to prohibit just that kind of thing: taping by a Government official for other than law enforcement purposes. I have reservations about totally uncontrolled one-party consent interception by anybody, including law enforcement, but that is too big a problem to tackle at this time. There are a great many considerations involved in that bigger issue and it is not necessary to deal with those to resolve this kind of problem which really does seem to occur. If the committee wishes, I can provide some language, I have already drafted some, and I tried to make sure it reaches only that kind of situation and not law enforcement taping.

I am aware, incidentally, of proposals to prohibit only the interception and disclosure, which focus on the disclosure aspect. Apart from raising memories of how poorly that combination worked in the old section 605, which you may remember, that approach doesn't get to the heart of the problem with consent taping, which is not that of privacy, but a problem of trust. One's privacy is almost waived, though only in part to be sure, when he or she reveals something to another person. The real issue, I think, is trust, the sense of betrayal when you learn that the person you are talking to is recording your words without your knowledge, regardless of whether it will be later disclosed.

Furthermore, the tape could still be used against the speaker without such disclosure, and it is that possible use which adds to the sense of betrayal which, I think, is very dangerous to a free society. Moreover, it is very hard to detect disclosure and this also adds to the sense of uneasiness and loss of trust.

I think we can handle the Wick situation without too much difficulty.

Computer and digitalization. I am not an expert in this field, but I have looked at 605, and I have some difficulty understanding some of the current concern about loopholes.

Title III seems clearly to reach all voice communications, no matter how transmitted and whether that be by analog or digitalization, which is what the telephone company is trying to install.

Section 605, second sentence, still applies to all radio communications that are not oral. Computer communications by microwave or satellite I should think are covered by this, though it probably doesn't catch fiber optics, which are wirelike, and any other kind of wire transmission.

Distinctions based on the particular transmission medium obviously make no sense, but until we think this problem through more than we have to date, it seems to me we do have something to reach at least some of these communications. Of course, the enforcement problem of detecting the interceptions would be very difficult.

I would add that I don't see how one can say that computer communications are not entitled to fourth amendment constitutional protections regardless of the statute, for I was sure there is an expectation of privacy when these are transmitted that the society should be prepared to recognize as reasonable.

My last comment is about title III. I can't let this occasion pass without expressing my dismay at the increasing use of wiretapping and bugging for law enforcement.

I have said my piece on this many times, probably to the intense boredom of at least some members of the committee and the general public, and maybe even my fellow panelists. I would nevertheless like to note with some alarm that a few weeks ago, it was reported that the number of title III installations in the first 9 months of 1983 reached 152, which is roughly a 200, annual rate, close to the second highest in history.

On a fiscal year basis, the 359 total of installed installations and extensions is a record, even for the fiscal years 1971 and 1972, when the antigambling Operation Anvil Project was in effect, now conceded to be one of the most wasteful law enforcement efforts ever undertaken.

This probably means that today more people are being wiretapped than ever.

Most of the increase is for drug enforcement and the amount of tapping will increase even more. It is being accompanied by the usual claims of success and indispensability, claims belied by history. Indeed, despite the National Wiretap Commission's finding in 1976 that wiretapping was effective, the staff found that it never reached the upper echelons in drug enforcement, and the drug authorities often refrained from its use until this Administration.

G. Robert Blakey, a member of that Commission, and author of the Wiretap Act, declared just a few months ago, after the Dorfman case, that prior use has been wasteful and inefficient.

Wars on drugs are continually being declared and wiretapping is continually invoked as indispensable. Yet, even though Bronx district attorney Mario Merola, one of the best district attorneys in

the country, told the Wiretap Commission in 1974 that he used it extensively for drugs—and only for drugs—he has used it only once in the last 5 years.

Indeed, the States' use of wiretapping has generally declined, despite the increasing number of States with wiretap authority.

I would add that the use of wiretapping in the ever-increasing number of RICO investigations is an especial cause for concern, since that statute is so vague and is being used so expansively that taps in such investigations will inevitably catch huge numbers of totally innocent people and conversations, far more than in almost any other kind of investigation.

Official electronic surveillance remains a distressing feature of modern America, and it will probably get worse. To many of us, the solutions are very inadequate and will become more so unless there is a basic change in official attitudes. Unfortunately, such changes seem highly unlikely at least at present.

Thank you.

[The attachments to the statement of Mr. Schwartz follow:]

[From the Nation, Oct. 29, 1983]

HOW DO WE KNOW FISA IS WORKING?

(By Herman Schwartz)

Every President since Franklin D. Roosevelt has abused the power to use electronic surveillance in national security matters. In an attempt to impose restraints on this power, Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA). Since the law was signed by President Carter five years ago this month, some stock-taking seems in order.

Like most reform legislation, FISA was passed in the wake of a scandal. When hearings in 1975 before Senator Frank Church's committee investigating intelligence agencies revealed the myriad outrages perpetrated by U.S. intelligence agencies in the name of national security, civil libertarians jumped at the all-too-rare opportunity to impose some controls. The Ford and Carter Administrations agreed to some restrictions for fear that outraged public opinion would impel Congress to impose stricter ones. After almost three years of intensive negotiations involving Congress, both Administrations and civil liberties groups, a compromise was hammered out that allows electronic surveillance in this country for the purpose of gathering intelligence about foreign powers and foreign agents. Under FISA, the Justice Department must obtain an order from one of seven specially designated Federal judges, who constitute a special court, authorizing any foreign intelligence electronic surveillance. Hearings on the government's applications are conducted in secret. The law forbids eavesdropping on American citizens, except if they are suspected of engaging in intelligence activities for a foreign power that involve violations of criminal statutes.

Since FISA took effect, the judges have issued authorizations for nearly 1,500 surveillances, but we have little idea of how well the law is working. What we do know, however, is disquieting.

For example:

During the nineteen months the Carter Administration used FISA, the government obtained 529 surveillance orders. Because some of them were extensions of earlier orders, it is difficult to determine how many bugs and taps were installed in those years. How many people were targeted and how many of them were Americans?

In 1981 and 1982, the first two years of the Reagan Administration, the number of surveillance orders granted by the judges to 433 and 475, respectively. Why? Were the additional taps and bugs used to eavesdrop on American citizens?

The judges have not denied a single government application. Is the special court a rubber stamp?

Reports of intelligence taps have surfaced in criminal cases, but the courts have done almost nothing to insure that FISA, which establishes looser procedures than

are required for criminal prosecutions, is not being used for law enforcement purposes.

Because the special judges' proceedings are secret, it is hard to evaluate how well they are doing their job. The statute called for annual assessments by Congressional intelligence committees for five years to determine how it is working, but Malcolm Wallop says that the Senate Intelligence Committee, of which he is a member, has never even "met to consider how FISA has functioned." Members of both the House and Senate committees have stated publicly that few Americans have been targeted, but the history of Congressional oversight in national security and foreign intelligence matters gives one little reason for confidence in those assurances. According to Senator Joseph Biden Jr., who gave some of those assurances, the Senate Intelligence Committee has never examined the special judges' authorizations in individual cases to determine whether the government's applications complied with the statute or whether the surveillance orders were properly issued; the House Intelligence Committee checked what it considered a "representative number" of authorizations and pronounced itself satisfied.

To shed some light on how the law is functioning, Representative Bob Kastenmeier of the House Judiciary Committee held hearings on June 8 and 9. Testifying were a judge of the special court, a Justice Department representative and Morton Halperin and Mark Lynch of the Center for National Security Studies. Not surprisingly, most of the testimony was not very informative. What information did emerge from the hearings was not reassuring, however.

The Justice Department representative, counsel for intelligence policy Mary Lawton, disclosed little of consequence. Judge George L. Hart Jr. of the Federal District Court for the District of Columbia, who served as the special court's first chief judge, refused to say very much, but his testimony was still revealing.

Hart's appointment to the court exemplifies one of the main problems with FISA—the judges themselves. The members of the special court were chosen by Chief Justice Warren Burger, who showed a preference for government-oriented judges like Hart and the present chief judge, John Lewis Smith Jr. Morton Halperin, who played a key role in the enactment of FISA, pointed out to the House committee that in making his appointments the Chief Justice did not consult as widely as he was expected to.

One indication of the special court's complacent attitude toward government requests for surveillance orders is the fact that it has authorized physical searches. Shortly after FISA went into effect on October 25, 1978, the Justice Department asked Judge Hart for permission to conduct such a search, even though the act applies only to searches by an "electronic, mechanical or other surveillance device." Hart readily complied—as did other special judges to subsequent requests. Upon learning of this expansion of the statute, the Senate Intelligence Committee criticized Hart and the other judges. After "further thought," as he put it, Hart decided he did not have the authority to issue break-in warrants after all. On June 3, 1981, the Justice Department sent him a formal memorandum along those lines, and a week later the judge issued an opinion declining the authority to authorize break-ins, which followed the reasoning of the memorandum.

At the Kastenmeier hearings, Judge Hart refused to answer almost every question of substance on grounds of national security. He showed great deference toward the Justice Department, praising the "dedicated personnel" there for doing a "wonderful job" on their requests for surveillance orders. It seems never to have occurred to him that a member of the department might abuse the law or try to stretch it. He seemed oblivious to the department's record of flagrant surveillance abuses under almost every President since Woodrow Wilson. It was the Justice Department, after all, that authorized the Federal Bureau of Investigation to tap and bug Martin Luther King Jr. That occurred under Attorney General Robert Kennedy, a nominal liberal. But Judge Hart seems to have long had a tolerant attitude toward the department. When Richard Kleindienst came before him in 1974 to be sentenced for having perjured himself in testimony to a Congressional committee about Richard Nixon's effort to influence the department's handling of the I.T.T. antitrust case, Hart imposed a \$100 fine and offered the Attorney General heaps of sympathy.

Judge Hart told the committee that the special court exercises no supervision after taps and bugs are installed. Consequently, there is no way of knowing if Federal agents observe the provisions in the act that limit the number of conversations they may overhear, record and disseminate to other Federal and state agencies and that seek to minimize the intrusiveness of a surveillance. Although FISA authorizes the judges on the special court to "assess the Government's compliance with the minimization procedures," Hart said that the court reviews only the Justice Depart-

ment's general procedures and does not seek to determine if the government has complied with the law in specific surveillances.

Judicial diffidence in the face of the government's national security claims is responsible for another worrisome development. Prior to 1978, when FISA was enacted, criminal defendants would not infrequently discover that they had been overheard on so-called national security wiretaps. The government always claimed that the taps had nothing to do with the criminal case, but in some instances that claim was ludicrous. In the F.B.I. investigation of the Jewish Defense League, for example, a massive "national security" surveillance on every telephone line in the group's office continued for a month after the start of a criminal prosecution for bombing the offices of Amtorg, a Soviet trading firm in New York City, and ended only after the existence of the taps was revealed by the government.

FISA procedures are less stringent than those under the act authorizing law enforcement wiretapping. The enactment of FISA has thus not eliminated the incentive to use intelligence gathering authority improperly to obtain evidence for criminal prosecutions. The few courts that have dealt with this problem have made it so easy for the prosecution to successfully deny misuse of FISA that in this respect the government is under no restraints at all. These courts have made their decisions turn on ascertaining the government's "primary purpose," an elusive standard at best. Since the decisions are made without any participation by the defendants, the judges hear only the government's side, without its being subjected to cross-examination.

Some trial court rulings on such evidence have been simply implausible. In a case involving I.R.A. gunrunning in this country, for example, a Federal court in Brooklyn held that evidence obtained by wiretaps authorized under FISA would be admissible because the government's "primary purpose" in obtaining it had been to collect intelligence information, not to prosecute American supporters of the I.R.A. Yet, for some time before the taps were installed, the U.S. government had been pressed by the governments of Ireland and Great Britain to bring criminal proceedings against Americans who were supplying guns to the I.R.A., and the targets of the surveillance were indeed indicted and tried.

Not even mentioned at the Kastenmeier hearings was the massive surveillance program carried out by the National Security Agency, which was exposed by the Church Committee and discussed in James Bamford's book *The Puzzle Palace*. In the early 1970s, the N.S.A. participated in President Nixon's war on drugs and worked with the Central Intelligence Agency under Operation Chaos to spy on protesters against the Vietnam War. For thirty years the N.S.A. ran its own surveillance program, known as Operation Shamrock, under which international cable companies turned over all their cable traffic to the agency. The information thus obtained was then disseminated to other Federal agencies, including the Justice Department, which used it in criminal prosecutions. N.S.A. surveillances touched not only suspected drug dealers but also antiwar activists, civil rights workers, Cuban exiles and such prominent Americans as Dr. Benjamin Spock, Joan Baez, Martin Luther King Jr. and Jane Fonda.

After the Church Committee exposed its illegal activity, the agency promised to mend its ways. But by taking advantage of loopholes in FISA, it is still engaging in electronic monitoring. The extent of its activities and whether they involve abuses like those committed in the past are not known, partly because the courts have blocked inquiries into N.S.A. procedures by allowing the government to invoke the "state secrets" privilege.

Obviously judicial scrutiny and legislative oversight of the administration of FISA are essential if the act is to achieve its purposes. Since there is no requirement in the act that targets of surveillance must be notified in all cases, there is little chance that anyone will challenge the legality of a tap or bug. Judge Hart's testimony, scanty as it was, provides little reassurance about judicial oversight. And Congress has not done what Morton Halperin has urged it to do: "insist upon a right of access, which . . . the statute clearly contemplated . . . insist upon seeing the full text of the whole record in some number of cases, randomly selected." Moreover, the annual reports by the House and Senate intelligence committees are no longer required by the act.

This is not to say there have been abuses. We just don't know. It may well be that most surveillance orders have been permissible under the law. The mere existence of FISA and its provisions for some external checks has probably forestalled some of the more egregious abuses. But the statute, with its elaborate provisions for judicial scrutiny and legislative oversight, was passed not just for easy cases but also for those where a careful look is both appropriate and necessary. As things stand, that hard look is missing.

TAPS, BUGS, AND FOOLING THE PEOPLE

(By Herman Schwartz)

III. NATIONAL SECURITY SURVEILLANCE

Where national security is concerned, privacy and confidentiality have rarely carried much weight. The CIA has opened hundreds of thousands of letters and screened millions more; the National Security Agency has intercepted millions of cables and international phone calls; the FBI, the military, the CIA, the IRS, and others have listened in on millions of phone calls in the United States involving countless numbers of people; the FBI, IRS, and others have perpetrated hundreds and perhaps thousands of burglaries; informants and agents provocateurs have been introduced into peaceful groups, often with tragic results for family, friendships, jobs, and health. All of this has been ostensibly for the purpose of obtaining intelligence to protect our national security against domestic and foreign threats, but all too often solely to stifle dissent.

Intelligence surveillance is even more indiscriminate and inclusive than law-enforcement surveillance. Where surveillance is directed to a crime, a specific criminal act or event provides at least some criteria for relevance and specificity. But where intelligence surveillance is concerned, there are few guidelines, and the "minimization" requirement becomes almost meaningless. As FBI Director Clarence Kelley said about foreign intelligence investigations: "In investigating crimes such as bank robbery or extortion, logical avenues of inquiry are established by the elements of the crime. The evidence sought is clearly prescribed by these elements. But there are no such guidelines in the field of foreign intelligence collection. No single act or event dictates with precision what thrust and investigation should take; nor does it provide a reliable scale by which we can measure the significance of an item of information. The value and significance of information derived from a foreign intelligence electronic surveillance often is not known until it has been correlated with other items of information, items sometimes seemingly unrelated. Also, difficulty in determining the potential value of information derivable from such an installation makes it hard to predict the required duration of the surveillance." The same absence of guidelines holds for the gathering of domestic intelligence, as the Supreme Court recognized in the Damon Keith case.

The Church Committee Report and discovery proceeding in court, especially in the on-going *Socialist Worker Party* Case, have now provided detailed confirmation of suspicions that national security taps and bugs have been used primarily for political and other illegal purposes. Virtually every intelligence agency, and many other government agencies as well, has violated the law again and again. Virtually every President since Franklin D. Roosevelt has approved, condoned, and often encouraged such violations. Attorneys General either ignored or encouraged. Congress deliberately chose not to know. Official lawlessness has been commonplace.

In 1941, Attorney General Francis Biddle approved a wiretap on the Los Angeles Chamber of Commerce as "persons suspected of subversive activities." Four years later, a high official in the Truman Administration and a former aide to Roosevelt were both tapped.

In the early 1960's Attorney General Robert Kennedy authorized, in the name of national security, an investigation of the sugar lobby, and approved taps on ten telephone lines of a law firm, three taps on executive branch officials, two on a Congressional aide, and a microphone in the hotel room of Harold D. Cooley, the Chairman of the House Agriculture Committee. The result, according to the Church committee, was "a great deal of politically useful information."

At the 1964 Democratic Convention, the FBI installed wiretaps and bugs on Dr. Martin Luther King, Jr., the Student Nonviolent Coordinating Committee, and on other civil rights organizations, and transmitted a great deal of information to President Johnson's aides about the Mississippi Freedom Democratic Party's challenge to the regular Mississippi delegation.

In an effort to destroy Dr. King, J. Edgar Hoover had the FBI install 16 taps and eight room bugs in Dr. King's hotel rooms and offices from the Fall of 1963 until his assassination in 1968; New York and Miami police also bugged Dr. King at the FBI's instigation, even in church. This produced thousands of hours of tapes, from which the FBI tried to disseminate allegedly damaging material to *Newsweek*, the *Los Angeles Times*, and other media. Tapes were also sent to Dr. King and to Mrs. King in what he and his aids considered an effort to drive him to suicide. The Church Committee concluded that "there is no question that officials in the White House and

Justice Department, including President Johnson and Attorney General Katzenbach, knew that the Bureau was taking steps "to discredit Dr. King."

President Nixon authorized taps on four journalist and 13 government employees, allegedly to ascertain the source of leaks on foreign affairs matters. The tap on one of these, Morton Halperin, was in effect 21 months, revealed no information relevant to leaks, was not based on any reasonable suspicion of him, was in contravention of internal Justice Department procedures, and was maintained for almost two years despite repeated reports soon after installation that it was producing nothing of value. The taps were also on White House staffers who had no contact with national security matters. Although producing no evidence as to leaks, the taps generated "a wealth of information," which was transcribed and turned over to the White House, "about the personal lives of the targets—their social contacts, their vacation plans . . . marital problems . . . drinking habits, and even their sex lives." In addition, purely political information was obtained from the phones of two targets who were advisers to Senators Edmund Muskie and Edward Kennedy. These taps on newsmen and executive officials were merely the successors to taps in the early and mid-1960's on other newsmen, including Hanson W. Baldwin of the *New York Times*, in an always futile effort to ascertain the sources of leaks.

Between 1975 and 1976, the CIA bugged Micronesian officials to learn their bargaining position in negotiations with the United States about the status of Micronesia.

These are but a few of many. Attorney General Edward Levi reported that from 1940 to 1975, the FBI alone had installed some 10,000 taps and bugs. This is probably but a small portion of the surveillance that actually took place, if one considers the activities of the CIA, the NSA, the IRS, the military, and some 20 other federal agencies which conduct electronic surveillance, about which Levi did not testify. The CIA, for example, has admitted tapping people it considered left-wingers both in this country and abroad, partly in something called Operation CHAOS, an effort to find links between anti-war groups in this country and foreign groups, which were never found; the National Security Agency has intercepted millions of overseas telegram and telephone messages; the military listened in on numerous radio messages in the late '60s and early '70s in connection with civil disorders and in full knowledge that such listening was illegal. And the FBI may not have reported all the taps and bugs it installed; in various court proceedings, such as the *Wounded Knee* and *Socialist Workers Party* cases, the courts have found that the FBI had lied about the existence of taps and bugs. In addition to all this, there are an unknowable number installed by local police "Red" squads, often at the instigation of federal officers.

All of this was done in the name of national security. In reality, it was aimed again and again at dissent and association. The FBI, for example, saw itself as "the guardian of public order" and established values, ordained "to maintain the existing social and political order." As the Church Committee put it, "the Bureau chose sides in the major social movements of the last 15 years and then attacked the other side with the unchecked power at its disposal." The very vagueness of the targets of FBI and other investigations makes this clear. The FBI and other national security agencies set up and indexed files and spied on people it considered "rabble rousers," "agitators," "subversives," "Black nationalists," "dissidents," "radical left," "new left," "extremists," "communist infiltrators," and the like. In many cases, these were citizens who simply disagreed with government policies.

And what was the primary purpose? To get names and to amass files on "enemies," people with whom the agencies were at "war." As one senior FBI official put it: "No holds were barred. We have used [similar] techniques against Soviet agents [The same methods were] brought home against any organization against which we were targeted. We did not differentiate. This is a rough, tough business."

* * * Legality was not questioned, it was not an issue.

The number of people and conversations overheard is incalculable, but it must be enormous. Figures supplied by the Justice Department a few years ago to Senator Edward Kennedy disclosed that in 1968-70, an FBI national security tap lasted on the average from 78.3 to 290.7 days, and this calculation is confirmed by information in the *Jewish Defense League* and *Halperin* cases, where the taps lasted many months and indeed years. Since Title III (i.e., law enforcement) taps average about 55 people and 900 conversations per 13.5 day interception, simple arithmetic indicates that each federal national security tap catches between 5,500 and 15,000 people per year. If one multiplies this figure by the hundreds of taps and bugs installed each year by the federal national security agencies, the figure comes to hundreds of thousands of people each year. Support for this huge figure comes from a few items developed in court cases. In the Detroit Weatherman case, for example, it

has been reported that one tape contained 12,000 separate conversations, many of them lawyer-client conversations.

All of this has been done with few if any external or internal controls. These agencies still lack a clear statutory base and use vague statutory language and executive orders and letters as authority. The law itself hasn't been clear. It wasn't until 1972 that the Supreme Court said intelligence surveillance for domestic security purposes on Americans without substantial foreign ties was unconstitutional, if full Fourth Amendment procedures weren't followed, though it held open the possibility that Congress could authorize a watered-down warrant procedure for domestic intelligence. Several lower courts have upheld foreign security surveillance without a prior warrant, though the District of Columbia Circuit intimated that it disagreed, and the Department of Justice seems to have accepted that court's ruling by proposing legislation that would establish a modified warrant procedure for foreign surveillance.

Nor are internal controls any more impressive, John Shattuck and Leon Friedman of the American Civil Liberties Union have given numerous examples and many details of the weakness of such controls. Former Attorney General Levi recently told of his bemusement when, on his first day in office, he was handed an application for national security tapping by an FBI agent and, as he saw it, was expected "automatically" to sign it. Levi seems to have imposed some guidelines, before departure from office; their present status is not known.

On a more technical level, the Church Committee found that screening out non-pertinent conversations was "extremely difficult, if not impossible." And, given the "vacuum cleaner" attitude of most intelligence agencies, an almost inevitable approach, given the broad and amorphous nature of "intelligence," it is difficult to see how it could be otherwise, especially where microphones are concerned, since "minimization" of microphone surveillance is always just about impossible.

What good has all this tapping and bugging of law-abiding Americans done? Very little. Although the primary purpose of all intelligence surveillance is supposed to be preventive, both the National Wiretap Commission and the Church Committee make it clear that such successes are rare indeed. The Wiretap Commission offered a few examples of successful prevention where domestic criminality is concerned, and the Church Committee simply said that preventive intelligence had occasionally been useful for national security, but it specified nothing about whether the electronic surveillance had contributed to that utility.

Many who have worked with national security surveillance have disparaged its value. Talking to John Dean on February 28, 1973, Richard Nixon said: "They [the taps] never helped us. Just gobs and gobs of material: gossip and bullshitting (untellible) . . . The tapping was a very unproductive thing. I've always known that. At least, it's never been useful in any operation I've ever conducted."

(In that respect, he wasn't totally accurate: the information that FBI picked up about a prospective article by Clark Clifford may not have promoted the national security, but it certainly was of political value to the Nixon Administration in countering opponents of its Vietnam policies.)

Ramsey Clark declared in 1972 that if all national security intelligence taps were turned off, the net adverse impact on national security would be "absolutely zero." Morton Halperin, a former staff member of the National Security Council, has taken the same position. CIA records disclosed that its microphone surveillance of Micronesian officials was "wholly unproductive," according to a Senate Intelligence Committee report in April 1977. The Court of Appeals for the Third Circuit found that the taps in one case had been "ineffective and unsuccessful," and the JDL taps did not prevent an Amtorg office bombing. The Church Committee concluded that wiretapping and bugging had been particularly useless with respect to discovering the sources of leaks, despite repeated use of electronic surveillance for this purpose by several Administrations. And many intelligence experts have consistently downgraded the importance of any kind of covert intelligence gathering. William F. Sullivan, former Assistant to J. Edgar Hoover for Intelligence, has even suggested prohibiting all electronic surveillance for a trial period of three years to see how we would manage; obviously, he doesn't think the Republic would totter during those three years. The Church Committee opposed electronic surveillance of Americans for purely intelligence purposes, and proposed that no non-consensual electronic surveillance of Americans be conducted except under Title III, with somewhat looser provisions for surveillance of foreigners, and an amendment of the espionage laws to include "industrial and other modern forms of espionage."

Cutting across all of this is a lesson history has taught again and again. From the Alien and Sedition Laws to Watergate, it is clear that executive power cannot be trusted, that it constantly identifies national security with personal political securi-

ty, and that especially in times of stress, the courts cannot be relied upon to curb it. Nor can we rely on good people in office. It really doesn't make much difference who is in power. Once in office. Jefferson, Lincoln, Wilson, Roosevelt, Truman, Eisenhower, Kennedy, and Johnson all committed grave violations of civil liberties when they felt threatened. No executive, caught in one of our perpetual domestic or international crises, can be expected to resist the temptation to use all the power at his disposal to fight criticism or obstruction of what he thinks he must do for what he may honestly consider the common good.

Any legislation to authorize intelligence surveillance must therefore be scrutinized very carefully, for the power it grants will almost certainly be stretched to the utmost. There is no reason to allow intelligence surveillance for *domestic* purposes, and neither the National Wiretap Commission nor the Justice Department has suggested it. Where *foreign* intelligence surveillance is concerned, no case has been made for going beyond the Church Committee recommendations mentioned above. Nevertheless, in 1976, Attorney General Edward H. Levi, Senator Edward Kennedy, and others proposed S. 3197, a foreign intelligence surveillance bill which goes considerably beyond the Church Committee proposals, and would allow wiretapping and bugging for foreign intelligence-gathering purposes of American citizens and resident aliens not chargeable with criminality. Apart from the wisdom of allowing any wiretapping on law-abiding Americans or resident aliens, the bill's procedural safeguards were meager: it gave the judiciary an oversight role much narrower than in Title III; it dispensed with even a representation by someone that the information sought is likely to be at the phone tapped or place bugged; it had a provision about Presidential power which some say denies the inherent power to tap and bug and others say implies its existence; and it did not cover interceptions by the National Security Agency of overseas communications.

Perhaps more important, the bill authorized electronic surveillance of people suspected of being involved in criminality without the protections of Title III, on the theory that the surveillance was only for intelligence purposes and not for criminal law enforcement. Attorney General Levi tried to distinguish sharply between intelligence and law-enforcement surveillances, in order to explain why fewer protections are needed for the intelligence variety. Regardless of the theoretical validity of such a distinction, in practice the two blur into each other. In case after case, so-called intelligence taps and bugs have turned up in criminal prosecutions. In the *Jewish Defense League* case, for example, a so-called intelligence tap was not only followed by an indictment, but was kept in operation for 30 days after the defendants were indicted. There are many other examples of the use of so-called intelligence taps for criminal law enforcement, but S. 3197 made no attempt to prevent such use. It could therefore be used as a device to circumvent Title III, which has much more stringent requirements than S. 3197.

In May 1977, the Carter Administration introduced S. 1566, a revised version of the bill which is better in some respects and worse in others. The ambiguous clauses about inherent presidential power to wiretap for national security purposes have been removed, from both the new bill and from Title III, and it is made clear that the two legislative acts are the exclusive means by which wiretapping and bugging may be conducted in the United States; NSA surveillance of messages emanating from the United States is covered; judges are given a little more authority (though still very little) to review the government's representations in its applications. On the other hand, the bill distinguishes sharply between American citizens and permanent resident aliens on the one hand, and temporary residents such as foreign visitors and students on the other, affording the privacy of the latter much narrower protection. The Constitution contains no such distinction, and it is unworkable as a practical matter: Electronic surveillance necessarily eavesdrops on the conversations of all who use a phone or talk in a room; and many of these will, in fact, be Americans.

Intelligence surveillance is something new in American law, and quite dangerous. Mechanically and legally, it is very difficult to control, especially where the investigations in which it is used are for such broad and vague purposes as national security or "foreign policy," as in S. 1566.

Nor dare we forget that more than wiretapping is involved. The electronic eavesdropping we authorize in the name of national security will not stop with that kind of "dirty business." The same justification has been applied to break-ins, burglaries, and physical violence by the intelligence agencies. It will be again.

Mr. KASTENMEIER. Thank you for that almost depressing conclusion, certainly. Thank you for your presentation.

Magistrate Carr?

Mr. CARR. It is a pleasure to be here. It is a particular pleasure to appear once again before Chairman Kastenmeier, for whom I worked, at least indirectly, in preparing the report of the National Wiretapping Commission several years ago.

I would like to address some of the issues which come out of the background of title III, how it happened to be written in the manner that it was, some of the problems that it has left for us, and some proposed, however tentative, solutions.

In an early article, an article which bears rereading by all of us, Professor Schwartz referred to wiretapping and bugging, electronic surveillance generally, as "omniverous," and I don't think there is a better one word description that can be used.

He also referred to title III as a "porous" statute, and indeed it is in many respects.

In order to understand title III and the problems which it creates for anyone who is involved with it, be it a prosecutor, a judge, defense counsel or private citizen, you should begin with the understanding, and never lose sight of that understanding, that title III was written to allow electronic surveillance, not to prevent it, although its structure is one of prevention or prohibition, subject to exception.

Prof. G. Robert Blakey was its draftsman and he had written a proposed electronic surveillance statute as part of his work with the Organized Crime Report for the President's Crime Commission in 1967. In many respects, that proposed statute predated title III and, indeed, predated the Supreme Court's *Berger* decision.

Professor Blakey's proposals remain unaltered, although many of the bases for those proposals were undercut by the Supreme Court decision in *Berger*.

In *Berger*, the Court held electronic surveillance, to be successful, must be conducted without notice to its subject; and in order to be constitutional, the waiver of notice that is necessary can be justified only if true exigency is shown to exist to justify the use of electronic devices. There is, thus, a key correlation between the absence of notice and the need for showing necessity.

In addition, the New York statute at issue in *Berger* was defective because it extended altogether too much authority to the officers executing the surveillance, and required too little judicial authority. And it did not require a showing of continued probable cause for extensions of the wiretap or bug and the prolonged duration of the use of the devices.

Nonetheless, following the *Berger* decision, Professor Blakey revised his proposals into the present form in which we have them. The statute takes only slight cognizance of the concerns which led the court to find the New York statute unconstitutional in *Berger*.

The duration problem remains with title III. A single wiretap order can permit surveillance to be conducted for 30 days, subject to further renewals for an indefinite period, although the average tap—and Professor Schwartz could probably correct my figures—but at least until a couple of years ago, the average Federal tap ran about 20 days, a little longer now.

That is not because of any inherent control within the statute itself. The exhaustion of alternative techniques requirement found in title III is, in my opinion as written, inadequate, and you are all

familiar with the absence of any clear specification about how minimization is to be conducted. Finally, with reference to judicial control, although Federal judges regularly are involved through the medium of periodic reports in oversight of electronic surveillance operations, that is because that is the way the Justice Department runs its operations, not because of any requirement in title III.

Title III permits that which would be permitted anyway; namely, periodic reports to the court. It does not require them. Judicial review to the extent it occurs today occurs because that is an internal approach and policy adopted by the Justice Department which, of course, could be changed with the next wiretap order.

In many respects, I am afraid that title III was written in a fairly haphazard manner. Professor Blakey wrote it while on the staff of the Senate Judiciary Committee. Senator McClellan indicated to him not to be too worried about the details of the statute and its rough edges, because when title III went to the House, there would be plenty of debate and plenty of opportunity for revision and so forth. That did not occur, so what was essentially a draft became a statute.

There are three ways in which law enforcement electronic surveillance can be adequately controlled.

One way is to limit it to a very, very small number of crimes, in other words, only narcotics, or only threats upon the life of a President, or only treason or whatever.

If you have but two or three categories of criminal offenses which are subject to wiretapping, it is not likely to be used with frequency, and you don't have to worry about the second way in which you can control wiretapping, and electronic surveillance, namely, through a rigorous set of procedural requirements which seek to make it difficult to obtain a wiretap order and see to it that there is adequate judicial control rather than prosecutorial control or control by the agents.

Finally, the third way in which you can control the extent of wiretapping is, of course, to regulate, much more stringently than the statute presently does, the period for which wiretapping can occur.

In my opinion, as a general rule, title III has adopted none of those three alternative methods of control. The Federal list of crimes which can be subject to a title III order is extensive and lengthy, and as Professor Schwartz notes, the opportunity to use wiretapping under the RICO statute opens all kinds of possibilities for broad and extensive wiretapping.

The authority extended to the State officials to wiretap, if their legislature extends that authority to them, is to wiretap or bug for any felony or other crime dangerous to life, limb or property. It is difficult for me to conceive of a crime which would not fit within that category, and consequently, State authorities have carte blanche to define the use to which they will put wiretapping and electronic surveillance under title III.

The procedures, the second category of control, the procedures as mentioned, are in my opinion loose.

The showing of necessity as presently prescribed is an inadequate protection.

It does not fulfill the policy, if not the mandate of the *Berger* decision, that true exigency be shown before these very dangerous devices can be approved and installed.

In terms of the success of title III, I have real questions whether title III has accomplished what its proponents said it would do, namely, to eradicate organized crime.

Certainly that has not occurred yet. Whether it does occur upon the marriage of title III and RICO remains to be seen. Title III has been only occasionally useful and the position and concerns expressed by the Wiretapping Commission represent the more accurate reading of the lack of success at that time.

Certainly, it has not been consistently useful in combatting organized crime. Those people frequently don't use the telephones and whether bugs could be more useful, I can't say. But talking as of today, the case has not been made that title III would accomplish what its proponents assured us it would accomplish: that is, that it would succeed in eliminating the existence and influence of organized crime in this country.

It can't do that because the constitutionally necessary restraints upon the use of wiretapping make it practically impossible to conduct the kind of surveillance which was successful in the 1950's, in the Manhattan District Attorney's office, which is frequently cited as proof that wiretapping can work.

It worked during that period because the wiretapping and electronic surveillance which was used then in New York City was totally unrestricted and not subject to the exclusionary rule. That is certainly not the case under title III. I would suggest to this committee to be very careful about citing ancient history about success, and what can be accomplished by title III.

Nor do I think that title III has been successful as it might in controlling excessive law enforcement wiretapping and at least avoiding, in an anticipatory fashion, the potential for abuse. The instances of abuse may have been slight, but that is not because of inherent strength within the statute. Professor Schwartz mentioned the decline in the use of title III type surveillance by the States.

I am not sure I would attribute that to its ineffectiveness. I think that has played a role. The principal reason that there is less and less State wiretapping and surveillance is the fact that it is an enormously expensive undertaking, and that indeed may be the only sure and certain protection against widespread electronic surveillance under title III: the cost of conducting these operations is enormous.

Six or eight or ten agents assigned on practically a full-time basis, monitoring the conversations, preparing amendments, initial paperwork, et cetera. The bureaucratic consequences are staggering, but also mandated not only by title III but by the constitution.

Therefore, the best protection that has existed for the past 15 years has been the demands made upon an agency by the costs of the operation. In many smaller cities, such as my own, Toledo, the Federal authorities simply do not have the kind of manpower to allocate to frequent and constant wiretapping operations.

I would like to take exception with Professor Schwartz on narcotics—this is an area to which surveillance can indeed be successful, subject to close monitoring.

People engaged in large-scale narcotics importation and distribution enterprises depend extensively upon telephone, radio and other kinds of oral communication, and it is more difficult for them to avoid a wiretap or a bug, simply given the nature of their operation and the need for immediate and instantaneous communication among the participants. Increasing numbers of cases have shown, Florida, New York, title III can be effective against large-scale narcotics operations. That success could, however, be accomplished with a more narrowly-drawn statute which is more limited than title III in its definition of offenses which are subject to electronic surveillance.

Regarding judicial control, the Federal Government has a procedure for reports every 5 days. That probably is too frequent given the paperwork and the demands upon the agents and the courts.

Every couple of weeks, every 10 days, would probably be adequate and it would give the agents and the supervising prosecutor sufficient time to ascertain whether an amendment is needed, whether or not minimization is adequate, whether or not the objective of the surveillance has been accomplished. At the same time, it would be less demanding upon the District or State judge. It would mean less time and more effective review by the judicial officer if these reports were required every 10 days or 2 weeks throughout the duration of the surveillance.

It would impose and underscore the need for judicial control as opposed to control by the agents of the executive branch.

I would also suggest that this committee consider strengthening the amendment requirement, particularly with reference to requiring amendment whenever probable cause arises about new people and their involvement. This is important because the statute requires notice only to those persons who are named in an application and order.

As other people are heard, if they are not included in successive orders, they will not necessarily receive notice that they were subjected to electronic surveillance, and even the proponents of wiretapping and bugging stress constantly the need for adequate notice to the people who have been overheard, that that has occurred.

I am concerned that under the present statute it does not occur to the extent that it should. This was pointed out by the Wiretapping Commission 6 or 7 years ago.

I would also suggest that it would be helpful in light of the *Donovan* decision to have a statement, if there is an amendment or are amendments to title III, to indicate the provisions, such as the notice provision, which play a central role in the regulation of law enforcement wiretapping so that their breach can lead to suppression.

Finally, with reference to the techniques which obtain information, not about spoken communication but other forms of communication, particularly pen registers, beepers, and video surveillance: the Supreme Court's decision in *Smith v. Maryland*, that the pen registers need not be preceded by a warrant, should be abrogated

by statute. There should be a requirement that pen register devices be preceded by a warrant or some showing of exigency or consent.

For many of us, the numbers that we dial are a reflection of ourselves and touch upon an interest of privacy that should be accorded protection but is not.

With reference to the use of beepers, again, the Federal Government has a policy and a practice of obtaining prior orders from people like myself, magistrates.

The Supreme Court has yet to deal directly with beepers, although it held in the *Knotts* case that a warrant was not required for monitoring a beeperized vehicle or trailer on a public highway. The Court has not addressed the question of beepers on private premises.

The Government has instituted on its own a policy of applying to magistrates for beeper orders. I see no reason why this could not be included as an amendment to title III, though there are some specific areas in which different kinds of showing should perhaps be made.

Nonetheless, it would be a fairly easy thing to do legislatively and an appropriate endeavor for this committee to undertake.

The Government does currently apply to magistrates for orders approving pen registers. That is an internal regulation and policy. But those orders are not directed toward the users of the telephone.

They are like the IRS enforcement subpoenas; that is, they are a way of getting approval from a judicial officer like myself to compel the production or the compliance with the request to install a pen register. In other words, it is directed to protecting the telephone company against charges that it is in cahoots with law enforcement.

Those orders are of an administrative nature, and they don't require a showing of probable cause. I have no discretion to deny such an order. They are intended simply to protect the telephone company and to enable the Government authorities to obtain the assistance of the phone company.

Finally, with reference to video surveillance, Mr. Beier of the committee staff called my attention to a recent decision involving a court-ordered video surveillance in Chicago.

This opens up an entire area of regulatory need and possibility, but upon superficial consideration in light of the small number of cases raising this question, again I think that video surveillance can be regulated through an amendment to title III, and it probably is appropriate that such amendment occur and within the confines of title III because, in fact, frequently video surveillance is used with audio surveillance simultaneously.

So that concludes my remarks, and once again I thank you for allowing me to be here.

Mr. KASTENMEIER. Thank you, Mr. Carr.

The third witness is Prof. Michael Goldsmith, currently with the New York State Organized Crime Task Force.

Professor Goldsmith, we have your 23-page statement, and if you care to abbreviate your comments, that statement will appear in the record.

Professor GOLDSMITH. Thank you, Mr. Chairman. I appreciate the opportunity that has been given to me to testify before this committee today.

I certainly will abbreviate my comments, as it would take quite some time to read a 21-page statement for you.

I am an assistant professor of law at Vanderbilt Law School, and I am on leave this year as counsel to the New York State Organized Crime Task Force.

However, the statements that I make today, as well as the statement that I have submitted, reflect my own views, not the views of the New York State Organized Crime Task Force.

Last year I wrote an article on title III. It was entitled "The Supreme Court and title III: Rewriting the Law of Electronic Surveillance." The thesis of that article was that, while, in fact, Congress, in enacting title III, had passed a statute which would both protect fourth amendment rights and advance law enforcement needs, the Supreme Court, through a series of decisions, has basically rewritten the statute with the result that fourth amendment rights often-times are not adequately protected.

The statement has been made here today by one of my co-speakers that title III is a porous statute.

I believe title III is both comprehensive and complex. This is not to say it is not in need of improvement. It clearly is. However, the statute is very complex. The real problem has been the lack of careful enforcement by the courts in their application of the statute.

I would ask the committee to approach the question of title III reform with great care. When the statute was passed, it was crafted in a manner designed to achieve a balance between law enforcement and fourth amendment rights. The National Wiretapping Commission Report, in essence, found that that balance had, in fact, been achieved. True, the statute had not achieved everything that its proponents had hoped. Nevertheless, progress was clearly being made.

Ironically, from a law enforcement standpoint, it can honestly be said that the main problem with title III has been its underutilization, not overutilization.

Professor Schwartz, no doubt, is cringing as I make these remarks. In truth, the use of wiretaps and bugs in the early 1970's for gambling prosecutions was a sorry waste of time. Clearly, the statute was not intended for that type of use. However, the statute was intended to attempt to eradicate organized crime. And I think that, far from criticizing the recent increase in electronic surveillance subject to court authorization, the Congress should be seeking increased use of electronic surveillance. Properly applied in the context of appropriate RICO racketeering cases, such increased use is, in fact, something that we should be trying to achieve. To the extent that there has been a decrease in enforcement or use of the statute by the States, I would attribute that to the comprehensiveness of the statute, its complexity, which has discouraged State officials from using it, as well, of course, as the great expense and time commitment that is required.

In terms of what can be done to improve title III, I think basically the following areas are deserving of close consideration by the

Congress. First is the area of standing, and by standing I mean, which parties under the statute are entitled to submit a motion before the court to suppress evidence obtained under the statute as having been illegally intercepted.

The broad language of title III, in fact, suggests that standing is to be conferred upon anyone who has been overheard, anyone whose facility, telephone or other facility is being used, or any person against whom the electronic surveillance is being directed. In other words, people who are not necessarily parties to the conversation are granted standing. And the purpose behind this broad standing language, in essence, is to prevent law enforcement from consciously violating the statute.

In a case, for example, in which law enforcement is listening to conversations between two named individuals the real target may be someone else, a higher echelon organized crime individual. Thus, without a broad standing provision, law enforcement may consciously say—and I do not say this is a practice of law enforcement—well, we will sacrifice the case against A and B presently speaking on the phone because we hope to make out a more important case against C, and since C is not named in the order and he is not speaking on the phone, he will not be in a position to assert that the evidence is inadmissible. However, because the judiciary has interpreted title III's standing provision too narrowly, such a scenario could occur.

I do not want to suggest that this type of abuse goes on in law enforcement circles. And I might add that, if that kind of abuse occurs, it is both a tort under the statute and a crime, a felony, and I would encourage prosecutors to initiate criminal prosecutions against people who have that kind of mindset. Likewise, I would encourage private citizens to bring civil suits against those who use the statute improperly.

Nevertheless, in order to protect all of us against the intrusions of electronic surveillance, the statute should be amended to conform to its original purpose. By that I mean that anyone against whom the electronic surveillance is being directed should have the right to file a motion to suppress the evidence.

How do you determine who the party is against whom surveillance is being directed? In this regard the statute already implicitly requires law enforcement to state its investigative objective. The statute, however, should be amended explicitly to require the objectives to be stated and the targets of the surveillance to be explicitly indicated. At the same time, the statute should contain limitations so that a broad standing provision does not taint an entire investigation by virtue of a single law enforcement violation.

The next area of potential reform has already been suggested by Magistrate Carr, and that lies in the context of exhaustion of investigative alternatives. Mr. Blakey, author of the statute, has given many speeches about the subject across the country. Incidentally, he should be consulted directly about how title III was written and its underlying legislative history. In any event, I have heard several of his speeches and he repeatedly says "electronic surveillance is a drastic technique." Because it is drastic, because it is so intrusive, it should, in fact, be something of last resort.

Now, that does not mean necessarily that law enforcement needs to try every other alternative potentially available. It does not mean that law enforcement should engage in futile measures to investigate crime, but it does mean that law enforcement should be making a good-faith, conscientious effort to use less drastic means than electronic surveillance before using the statute.

As an aside, I might point out that, while it is often said that electronic surveillance is the most intrusive means of conducting a search, on its face that seems to be a reasonable statement. At the same time, we should recognize that when law enforcement gets a search warrant and they search your home, the nature of that search, in fact, can be horribly intrusive, much more so than electronic surveillance. Of course, the difference is that it is not being conducted over a great period of time, but nevertheless, the search of one's home or one's office is, in fact, a drastically intrusive search. Depending on the terms of the search warrant, virtually everything in the house can be looked into.

In any event, what I would recommend in the context of the exhaustion requirement is that the statute be amended to require law enforcement to specify that virtually every aspect of a checklist set forth in the statute—by amendment—has been complied with. In other words, law enforcement would have to take a look at whether or not a pen register was tried, whether or not a search warrant was obtained, whether or not grand jury techniques were used, et cetera, et cetera, and, when a specified technique was not used, law enforcement should make an effort to explain why the particular technique was not used.

Now, I don't think that that type of requirement should be applied rigidly, but I do think it should be applied reasonably and that would force law enforcement to consider alternatives and it would force the courts to look at the adequacy of the exhaustion statement set forth in the application. Presently, too often the exhaustion statements are simply boilerplate. They are a conclusory statement that investigative alternatives have been tried and have failed, or simply that investigative alternatives are not available. Plainly that is not the full and complete statement that is required by the statute presently. In order to ensure that we do get the right kind of statement, the statute should be amended.

Next, in the area of the scope of surveillance, considerable concern has been expressed today about the wide-ranging nature of electronic surveillance. The first area deserving of consideration is whether surveillance should be permitted of unnamed parties. Now, clearly the statute permits interception of conversations between a named party and an unnamed party. However, by virtue of Supreme Court decisions, specifically the *Kahn* case and the *Donovan* case, the statute has also been interpreted to apply to surveillances between unnamed parties, people that were not specified in the warrant. The impact of this, if you will, is to open very significantly the range, the breadth of electronic surveillance.

My suggestion, for reasons I specify in much more detail in my statement and in my article, is that the statute be amended to require specification of all parties for whom there is probable cause to believe interception is going to occur. In addition, once the statute does include such a requirement, prosecutors should, in fact, be

required to amend as soon as there is probable cause for new parties. I might add that the process of amending and dealing with the courts is extremely time consuming, extremely intricate. When you are involved in a wide-ranging electronic surveillance, you could come across numerous parties. For that reason, while the requirement should be added, it should be flexibly applied.

The next area involving the scope of electronic surveillance deals with the so-called minimization requirement. Specifically the statute requires that the surveillance be conducted in a way that minimizes the interception of nonpertinent conversations. In fact, that requirement has not been effectively applied by the courts. The courts typically have been applying the minimization guidelines that have developed very liberally, without really carefully analyzing whether, in the context of a particular case, minimization could have been achieved. Second, in the Supreme Court's *Scott* decision a few years ago, the Court said that minimization violations are going to be evaluated objectively rather than subjectively, meaning that the good or bad faith of the law enforcement officials attempting to minimize is not considered in evaluating whether a violation has occurred.

That aspect of the statute was probably mistakenly interpreted by the court. In any event, it should be changed. We should clearly be encouraging agents conducting surveillance to be acting in good faith. And I might add that this is usually the case. I have seen Federal and State agents being instructed by prosecutors on how electronic surveillance is to be conducted and they are told to be conducting it in good faith. They are further told, from my own experience, that, should they at any time exercise bad faith, they will, in fact, be removed from the wire. Furthermore, on occasion, if there is bad faith resulting in a violation, it would not be unusual for a prosecutor to make that fact known to the court in his progress report.

The next area of concern has to do with amendments for new crimes. The statute presently has, in effect, what is a plain view section; should evidence of a new crime come into plain view, prosecutors are required to amend the warrant retroactively by filing an amendment before the court indicating that evidence of new crime has been detected. The courts have, however, not applied that section of the statute very carefully. Prosecutors are required to amend under the statute as soon as practicable. In fact, they typically have not done that. In candor, that is sometimes a difficult thing to achieve since it is not always clear when you have probable cause to believe that a conversation pertains to a new crime.

Some courts have interpreted the amendment requirement with undue rigidity, however. They have gone to the other extreme. For example, there are situations in which a conversation happens to pertain both to a crime specified in the warrant and to a new crime. The same conversation, in other words, is probative both of a crime mentioned in the warrant and some other crime. Under those circumstances, no purpose is served by requiring an amendment. It is silly. It is time consuming.

For example, assume you are in a wire for robbery and a conversation is intercepted in which the very same words pertain both to

robbery and kidnaping. Since that conversation pertains to the original crime specified in the warrant, there is no plain view consideration that comes into effect, and, therefore, no benefit to be obtained by requiring law enforcement to seek a retroactive amendment under those circumstances.

The next area of major concern should be the area of progress reports. In fact, as a general rule, the courts are not carefully evaluating progress reports. Consequently, you have potential for surveillance being approved initially based upon probable cause, however 2 or 3 weeks into the wire there is no evidence that is incriminating, nevertheless either because no progress report has been filed, or because the report has not been properly evaluated, the judge may not be aware of the fact that probable cause, in effect, has dissipated. The statute should be amended to require mandatory progress reports, either once a week or once every 2 weeks, in which prosecutors are required essentially to set forth what has been achieved so far. In other words, do we still have probable cause for the surveillance? Furthermore, if we have achieved a sufficient number of incriminating conversations, perhaps our investigative objective has been attained, and accordingly, there is no longer a need for continued surveillance.

Mandatory progress reports would also achieve the purpose of dealing with how evidence of new crimes should be handled by law enforcement. As soon as there is probable cause to believe a conversation pertains to a new crime, the progress report requirement should be one that compels that the new crimes be specified therein. And finally, progress reports can be useful to the judge in evaluating whether minimization has been properly implemented by law enforcement.

The present statute is one that only provides for optional progress reports. As a reform, title III should make them mandatory.

Next, the area of sealing. Much has been said about the sealing of tapes. The statute requires that the tapes be sealed at the end of the surveillance period, immediately upon the expiration thereof. Sealing, however, is very silly stuff. There is no magic to a seal. A seal is simply a piece of Scotch tape that you put around the tape.

People originally were concerned about tape recordings being tampered with. If someone has the sophistication to tamper with a tape recording—and that is very much open to question—but if someone has the sophistication to do that, he certainly has the sophistication to take off the Scotch tape and replace it with another piece of Scotch tape. Therefore, what I would suggest is complete elimination of the sealing requirement. Law enforcement already has to establish the accuracy of the tapes as a prerequisite to their admissibility. However, should there be concern and for some reason you decide to retain the sealing requirement, it should probably be changed from the language presently used in the statute. As I said, presently law enforcement has to turn over the tapes to the judge for sealing at the end of the surveillance period. The surveillance period usually is 30 days. That gives, in theory, 30 days for someone to forge the tape. So I would suggest that the sealing requirement be changed to 72 hours after the tape has been used. That gives law enforcement plenty of time to process the tape as it

must and at the same time gives the litigants involved and the people under surveillance adequate protection.

Mr. Chairman, I would rely upon the remarks I have made in my formal statement to supplement the remainder of my testimony. I realize that we are pressed for time.

One final comment is in order. If you are going to make title III more comprehensive, more complex, and I believe the statute should be reformed, we will all benefit by that. At the same time, I don't think that the original balance between law enforcement and fourth amendment rights should be modified. I would also recommend that should the Supreme Court adopt the good faith exception to the suppression rule for fourth amendment violations, that the good faith exception likewise be included in the statute.

I very much appreciate your time today. Thank you.

Mr. KASTENMEIER. Thank you, Professor Goldsmith.

[The statement of Mr. Goldsmith follows:]



STATE OF NEW YORK
 ORGANIZED CRIME TASK FORCE
 226 Westchester Avenue
 White Plains, N. Y. 10604
 (914) 682-8700

RONALD GOLDSTOCK
 Deputy Attorney General

Northern Regional Office
 Empire State Plaza
 Agency Building #1, 9th Floor
 Albany, N. Y. 12223
 (518) 474-1820

Western Regional Office
 Ellicott Square Building
 295 Main Street
 Buffalo, N. Y. 14203
 (716) 847-3457

January 20, 1984

Mr. Robert W. Kastenmeier
 Chairman, Subcommittee on Courts,
 Civil Liberties and the
 Administration of Justice
 U.S. House of Representatives
 Committee on the Judiciary
 Washington, D.C. 20515

Dear Congressman Kastenmeier:

Thank you for inviting me to testify before the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice. Enclosed are copies of a draft of my statement. Your staff counsel, David Beier, has advised me that I will have the opportunity to make revisions and provide you with footnotes within the next few weeks. As my court schedule is extremely heavy, I appreciate this extra leeway.

Sincerely,

MICHAEL GOLDSMITH
 Counsel

MG/sp
 enclosure

Goldsmith

(DRAFT)

A Statement for the Reform of Federal Eavesdropping Legislation

By Professor Michael Goldsmith

I would like to thank the Judiciary Committee of the United States House of Representatives for inviting me to express my views on the subject of electronic surveillance. Presently, I am an assistant professor, on leave from Vanderbilt Law School, serving as Counsel to the New York State Organized Crime Task Force. My testimony today however, represents my views alone rather than those of any institution.

My understanding is that the Committee would like me further to develop aspects of an article that I recently authored entitled The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance, 74 J. Crim. L. & Criminology 1 (1983). More specifically, I have been asked to provide suggestions for reforming Title III, the federal law which governs the use of nonconsensual electronic surveillance in this country. Given the thesis of my article -- that the Supreme Court has, in effect, rewritten Title III through a series of decisions which deviated from the Court's original guidelines for the enactment of a constitutional eavesdropping statute -- legislative review of this issue is certainly appropriate. Significantly, previous efforts at legislative reform, such as S. 1630 introduced before the 97th Congress, sought to effect significant improvements, but failed to realize the extent to which Title III has been modified by decisional law.

Accordingly, this statement will set forth a series of proposals for reform of Title III. For the most part, these proposals were either explicitly or implicitly made in my article. Since I cannot hope to duplicate in this statement the detailed analysis contained in a 171

page article emphasis of key points rather than comprehensiveness of analysis will be my primary goal. For more detailed analysis, citations to my article or to other sources have been provided. Finally, please note that, as I have had the benefit of both additional experience and collegial commentary since the article was published, some of the proposals are modifications of those which I originally made.

I have organized my remarks to emphasize the six areas I believe are most deserving of legislative attention: 1. Standing to Contest Title III Violations; 2. The Need to Exhaust Investigative Alternatives; 3. Controlling the Duration and Scope of Interception; 4. Preserving the Sanctity of the Tapes; 5. Emergency Searches; and 6. Standards of Review and Suppression for Title III Violations. My discussion of each area will usually include both civil libertarian and law enforcement concerns, for each perspective must be meaningfully considered if Title III is to be properly revised. As such, law enforcement supporters must acknowledge the legitimate concerns of those who fear the intrusiveness of an electronic search; likewise, civil libertarians must concede that court authorized electronic surveillance is a reasonable way, indeed, the only way, to combat effectively the severe social and economic consequences wrought upon our society by organized criminal groups. Title III is already an extraordinarily complex piece of legislation that the National Wiretapping Commission recognized as having afforded law enforcement with a vital investigative tool while simultaneously preserving Fourth Amendment rights. In considering reform, great care must be exercised to avoid imposing requirements that would make resort to electronic surveillance unduly burdensome or effect

the suppression of evidence for every sort of statutory violation. Constitutional rights are, in fact, advanced through a system that discourages police misconduct by providing a reasonable way to achieve investigative goals legitimately. It is with this sense of balanced perspective that I urge the Committee to evaluate the proposals which follow.

1. Standing to Contest Title III Violations

By legislative design, standing to contest alleged Title III violations is a prerequisite to the availability of the statute's evidentiary suppression remedy that is intended to deter misconduct. In this regard, Title III appears to grant claimants the benefit of a liberal standing rule by defining the term "aggrieved person" as "a person who was a party to any intercepted wire or oral conversation or a person against whom the interception was directed" (emphasis added). Yet, although this broad language seems to confer so-called target standing upon potential litigants, by authorizing anyone "against whom the interception was directed" to raise a suppression claim, the Supreme Court has effectively restricted Title III standing to intercepted parties or anyone whose telephone or facility is the subject of surveillance. Unfortunately, this effect was achieved as a result of some dicta, rendered in Alderman v. United States without the point ever having been briefed, suggesting that Title III standing was quite limited in scope. The Alderman dicta, however, was inconsistent with the statutory definition of "aggrieved person", and ignored a substantial body of legislative history which seemed to indicate that target standing was intended by Title III's authors. Admittedly, the Supreme Court has recently rejected target standing in the constitutional law context, but that ruling

obviously has nothing to do with the legislative intent underlying Title III at the time of its enactment.

As a policy matter, it should be apparent that target standing is the only practice which squares directly with Title III's goal of deterring illegal electronic intrusions. Simply put, absent target standing, prosecutors and police are relatively free to tolerate or even encourage misconduct in those situations in which the intercepted party (or facility) does not involve the target of the investigation. Under such circumstances, law enforcement may have incentive to violate the rights of suspected lower echelon criminals -- secure in the knowledge that higher echelon investigative targets will not be in a position to assert a Title III claim. While such conduct by law enforcement officials would potentially expose them to statutory criminal and civil liability, Title III's criminal and civil provisions have rarely been utilized. Fortunately, no evidence has emerged of such prosecutorial misconduct, but, to avoid this occurrence, the statute should be specifically amended to provide for target standing.

Any such amendment, however, should give ample consideration to law enforcement's legitimate concern that blanket target standing may have disproportionate consequences if a violation which directly affects a few individuals is permitted to taint subsequent investigations as well. Not all violations pose such a risk, but the potential nevertheless exists. This risk, however, can be minimized by requiring law enforcement authorities to specify their investigative objectives and targets in the eavesdropping application. Arguably, the statute already implicitly requires a statement of objectives in order for a reviewing

magistrate to assess the investigative need for surveillance and the duration for which eavesdropping is to be authorized (concepts which are discussed in sections 2 and 3 below), but many applications make no specific reference to investigative objectives. Adoption of such a requirement would allow the scope of standing to be determined directly by reference to the eavesdropping application. This requirement would also have the advantage of motivating law enforcement officials to state their investigative goals conservatively, thereby often narrowing the scope and duration of surveillance. Any problems involving subterfuge omissions could be handled by piercing the statement of objectives and targets, with standing being extended to persons for whom there was reasonable cause to believe involvement in the activity under investigation. Excessive taint should not occur for, as with inaccuracies in traditional search warrant affidavits, the burden of establishing an intentional or reckless misstatement would lie with the defendant. Finally, traditional attenuation principles would still operate to limit undue consequences of the suppression sanction.

Finally, there is an aspect of standing in the grand jury context that merits reform. In Gelbard v. United States, the Supreme Court correctly interpreted Title III to provide a just cause defense for grand jury witnesses who seek to avoid the contempt sanction by arguing that their refusal to testify is predicated upon questioning derived from illegal electronic surveillance. Gelbard, however, failed to provide guidance concerning the extent to which court authorized surveillance must be disclosed to the witness during the course of resolving such claims, and lower courts have since been divided. While

the language of Title III presently seems to mandate limited disclosure to the witness, I believe that no such access should be allowed. Given the relatively limited extent of present disclosure, little is accomplished towards protecting the witness' constitutional rights that could not adequately be achieved by in camera judicial review. Moreover, few recalcitrant witnesses are concerned with vindicating their Fourth Amendment rights. Historically, most such witnesses (other than victims of crime whose recalcitrance typically reflects safety considerations) are anxious for purely tactical reasons to learn whether their questioning is derived from electronic surveillance. If so, the witness will usually attempt to tailor his testimony carefully to what he believes the prosecutor already knows; if not, the witness often realizes that he has, in effect, a license to lie. In camera judicial review, with the witness merely being advised that his questioning is not based upon illegal electronic surveillance, will avoid this result.

Admittedly, since this proposal is based upon the limited disclosure presently authorized by Title III, some might argue that my premise would be undercut if the statute were amended to provide for complete disclosure to grand jury witnesses. Such an approach, however, would inevitably embroil grand jury inquiries in lengthy suppression hearings, a consequence fundamentally at odds with efficiency considerations that have long governed grand jury procedure in our society.

2. The Need to Exhaust Investigative Alternatives

In providing guidelines towards the enactment of a constitutional eavesdropping statute, the Supreme Court strongly suggested that resort to electronic surveillance should not be permitted when less drastic

investigative alternatives are available. This viewpoint was incorporated into the statute by the requirement that each surveillance application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." While Congress intended this requirement to be applied in a common sense manner so that law enforcement authorities should not feel constrained to expend time and resources on obviously futile investigative efforts, the statute plainly calls for a "full and complete statement" from which the reviewing magistrate can realistically assess the need for surveillance. Oftentimes, however, this requirement has been deemed satisfied by boilerplate assertions that investigative alternatives have been exhausted. Relatively few opinions have carefully analyzed whether the exhaustion statement is full and complete, much less whether it is based on substance. A probable consequence is that electronic surveillance occasionally has been approved when less drastic means may have sufficed.

The present situation can be ameliorated by an amendment requiring that the exhaustion statement contain, in effect, an investigative checklist (as set forth in the revised statute) of every alternative reasonably available and an explanation of its inutility. This amendment should likewise be interpreted in a common sense fashion, as its purpose is not to encourage futility (nor should suppression necessarily follow because a particular technique was not used.) Rather, it would serve to ensure that the judiciary has been provided with an adequate factual basis to evaluate the need for an intrusive electronic search. Furthermore, given the need to supply such a statement, it is likely that law enforcement will file fewer unnecessary applications.

Finally, the requirement of a statement of objectives (see section 1) should be regarded as a corollary to this improved exhaustion statement. Indeed, absent a statement of objectives, neither investigative need nor the proper duration for eavesdropping authorization can be realistically appraised. For this reason, specificity of objectives is already an implicitly required component of the exhaustion statement. Nevertheless, since many eavesdropping applications have not been sufficiently specific in this regard, an explicit requirement to this effect should be adopted.

3. Controlling the Duration and Scope of Interception

A. Surveillance of unknown parties

A major point of controversy in the Congressional debate over electronic surveillance concerned the number of persons potentially subject to eavesdropping. In an effort to limit the scope of interception, Title III seemingly limited surveillance to identified persons for whom there was probable cause to believe participation in specified discussions of criminality. While the statute clearly contemplated such persons inevitably being overheard in conversations with unknown individuals, it apparently did not countenance long term interception of discussions exclusively involving unidentified parties. Thus, just as traditional search warrants operate to protect the rights of unknown third persons by requiring the object of the search to be identified, Title III was designed to protect this category of individuals by limiting surveillance to conversations involving at least one identified person.

This protective mantle of Title III was undercut by Supreme Court dicta in United States v. Kahn and United States v. Donovan

suggesting that eavesdropping warrants may authorize surveillance of specified persons "and others as yet unknown." The dicta was grounded in the notion that "[t]he Fourth Amendment requires a warrant to describe only 'the place to be searched, and the persons or things to be seized,' not the persons from whom things will be seized," a narrow constitutional construction fundamentally at odds with the well established principle that "the Fourth Amendment protects people, not places." Apparently, the Court had failed to consider that specificity of party in an eavesdropping order is necessary to provide unknown third persons with constitutional protection equivalent to that which they are entitled under a traditional search warrant. Moreover, even though Title III's legislative history indicates that Congress appreciated the need to protect unknown third parties, and, accordingly, limited the scope of interception to conversations involving at least one known individual, the Kahn Court proceeded to suggest that surveillance against exclusively unknown persons was statutorily permissible as well.

To restore the proper protective scope to Title III, an amendment should be adopted restricting eavesdropping to conversations involving at least one identified party. Conversations between unknown persons should not be subject to interception unless probable cause exists that virtually everyone using the designated facility or telephone is doing so for the illicit purpose set forth in the warrant. An exception should also be allowed for the early surveillance period when monitoring agents are in the process of becoming familiar with the voices of their targets; moreover, provision should be made for anyone intercepted "in plain view" during this period to be expeditiously added to the eavesdropping

warrant. For example, such amendments should be permitted without additional Attorney General approval or the need to exhaust investigative alternatives (Cf. section 3.C below). In this way, the present scope of interception can be substantially narrowed without unduly impeding effective law enforcement.

B. Minimization of nonpertinent conversations

In a further effort to limit the scope of interception, Title III requires that "the authorization to intercept...shall be conducted in such a way as to minimize the interception of [nonpertinent] communications ..." (emphasis added). Accordingly, monitoring agents are not permitted to intercept conversations not relevant to the target, crime, and conversation specified in the eavesdropping warrant. While perfection obviously cannot be expected--some interception being inevitable as the monitor listens to determine pertinency--minimization was perceived as a reasonable way to discourage eavesdropping not relevant to the court order. Indeed, when the Supreme Court commented in Kahn on the permissibility of intercepting "others as yet unknown," the minimization requirement was cited as providing an adequate safeguard against sweeping general searches.

Unfortunately, however, the minimization principle has often been given minimal effect. In part, this may be attributed to the courts' willingness to apply judicial minimization guidelines too uncritically; consequently, minimization violations are rarely found (this tendency may be reversible by a Congressional directive calling for strict enforcement; see section 6 below). But, more fundamentally, by virtue of the Supreme Court's decision in Scott v. United States,

monitoring agents are, in effect, encouraged to seize any conversation whose interception can be justified under existing guidelines -- regardless of whether the conversation is actually nonpertinent. Scott held that, notwithstanding the monitoring agents' purposeful failure to initiate minimization efforts, no violation has occurred if the resulting seizure is still viewed as objectively reasonable under prevailing minimization guidelines. Thus, subjective bad faith is not considered in determining whether the minimization requirement has been violated.

From a statutory perspective, Scott was wrongly decided, and, therefore, should be legislatively reversed. The decision disregards the Congressional directive that eavesdropping orders be "conducted in such a way as to minimize interception of [nonpertinent] communications" (emphasis added). Moreover, if subjective good faith is not required when executing an eavesdropping warrant, the statute's broad deterrent purpose is effectively undermined. Indeed, Scott seems to have tolerated conduct which was actually felonious under Title III's criminal sanctions. Therefore, to reinvigorate the minimization requirement, an amendment should be adopted providing that alleged violations be considered from both an objective and subjective standpoint.

A related problem in the minimization context is the extent of suppression that should be mandated when illegality has occurred. Most courts have limited suppression to the improperly minimized conversations themselves. This solution, however, does not sufficiently penalize violators, since law enforcement loses only that to which it was never entitled; moreover, such conversations are often innocent discussions that are not relevant to a criminal prosecution. Nevertheless, at the

other extreme, total suppression would be a disproportionate remedy, as isolated minimization violations should not be allowed to taint an otherwise proper long term investigation. A suitable legislative compromise would be one that establishes a middle ground between these two alternatives. For example, an appropriate accommodation might focus on whether the minimization violations constitute a pattern of illegality. If so, all conversations seized during the course of that pattern should be suppressed (e.g., all calls intercepted on a particular day or by a particular monitor). Moreover, if multiple patterns -- suggestive of recklessness or intentional misconduct -- occur, total suppression would be in order. This remedy would provide an adequate disincentive against minimization misconduct without unnecessarily jeopardizing an entire investigation.

C. Retroactive and prospective amendments

While Congress was concerned about limiting the scope of eavesdropping, it recognized that monitoring would often expand beyond the crimes specified in the warrant. Indeed, assuming that proper minimization techniques are being employed, discovery of new crimes is a desirable consequence of electronic surveillance. By analogy, as officers executing a standard search warrant may properly seize unanticipated evidence that comes into "plain view," surveillance monitors may unexpectedly come upon conversations involving criminal activity not described in the court order. Title III allows evidence of such crimes to be admissible "when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of

this chapter. Such application shall be made as soon as practicable." Thus, a statutory plain view procedure has been established providing, in effect, for retroactive amendment of the original eavesdropping warrant once the interception's propriety has been judicially determined. Arguably, this procedure exceeds constitutional demands, as the Fourth Amendment does not require a comparable retroactive amendment "as soon as practicable" for conventional search warrants that result in plain view seizures; instead, the propriety of the seizure awaits determination at the eventual suppression hearing.

Regardless, few courts have enforced Title III's requirement that retroactive approval be sought as soon as practicable. This tendency, which may be due to the difficulty of determining practicality, could be easily rectified by requiring that, to the extent realized, evidence of new crimes be set forth in weekly progress reports to the magistrate who issued the warrant (see section 3.D below). At that time, the judge could rule on the propriety of the interception, but he should also be allowed to defer judgment until the pretrial suppression hearing when the full context of the case can more effectively be presented to him.

The more serious omission in this area has been the judiciary's failure to evaluate critically the admissibility of new crime evidence under traditional Supreme Court guidelines for plain view seizures: 1. whether the initial intrusion was valid; 2. whether the conversation's incriminating character was "immediately apparent;" and 3. whether the discovery was inadvertent. Together these guidelines were designed to ensure that law enforcement does not use the plain view concept as a

pretext for effecting general searches. Because this standard may be constitutionally required, its enforcement would be advanced by specific incorporation into the statute. However, as the Supreme Court has suggested that the plain view doctrine may soon be revised, any amendment should await, or be subject to, such modification.

From a law enforcement standpoint, the retroactive amendment requirement has occasioned serious difficulties in some circuits that have interpreted the provision too rigidly. These courts have suppressed evidence by holding that the procedure applies even to statements which happen to pertain both to the crime specified in the warrant and some other offense. Since, under such circumstances, the intercepted remarks are already within the terms of the eavesdropping warrant, the propriety or scope of the seizure requires no further clarification. By analogy to conventional searches, the situation is equivalent to a seizure by warrant of a suspected homicide weapon which is later determined to pertain to a separate robbery incident as well. Since Title III clearly was not intended to require retroactive amendments in such situations, legislative reversal of the offending decisions is in order.

Finally, implicit to Title III is the requirement that a prospective amendment to the eavesdropping order be obtained as soon as there is probable cause that new crimes will be intercepted. This mandate is a consequence of the inadvertence component to the plain view doctrine. More specifically, since inadvertence for plain view purposes is defined objectively as the absence of probable cause, retroactive amendments may be approved only when there was no probable cause to believe that evidence of new crimes would be overheard. Therefore, when

the requisite probable cause exists, a prospective amendment should immediately be obtained as the interception can no longer be justified on traditional plain view grounds.

This process, however, places law enforcement in an intractable dilemma: if a prospective amendment is issued, defense counsel will argue the absence of probable cause; conversely, if no such amendment is obtained, defense counsel will contend that plain view retroactive approval should not be granted because there was probable cause to anticipate the interception of new crime evidence, and, therefore, a prospective amendment should have been sought. Moreover, there are further difficulties for the prosecutor who seeks a prospective amendment. Because the statute does not expressly require such an amendment, there are significant questions concerning which procedural requirements are prerequisites to its issuance. For example, must the Attorney General (or designated Assistant Attorney General) approve such applications in the same manner required for the original eavesdropping application? If so, bureaucratic delay will inevitably preclude timely amendments. Also, must the exhaustion mandate be satisfied as to the new crimes evidence? If so, valuable evidence may be lost by requiring monitors to terminate interception when the conversation turns to new areas of criminality. Finally, may a prospective amendment be obtained when the new crime is not one of those authorized by statute for interception.

Perhaps for these reasons, the courts have largely ignored the prospective amendment concept. Nevertheless, since the inadvertence aspect of the plain view doctrine is probably of long term constitutional vitality, a specific statutory procedure should be provided for addressing

these problems. The procedure adopted should be sufficiently accommodating to the difficulties outline above. Thus, for example, where good faith has been exercised and a prospective amendment obtained, probable cause should be flexibly and reasonably interpreted; alternatively, perhaps a modified "inevitable discovery" doctrine could resolve the prosecutor's dilemma. As to Attorney General approval, exhaustion, and non-designated crimes, flexibility should likewise be the key. Under such circumstances, judicial review of probable cause and the nature of the offense is sufficient to safeguard Fourth Amendment rights. Additional protection could be secured by requiring retroactive Attorney General approval within ten days of the prospective amendment's issuance. In this manner, the statute could be brought into constitutional conformity without precluding effective law enforcement.

D. Mandatory progress reports

Since Title III is substantially premised upon close judicial supervision of electronic searches, a final precaution against improperly expansive eavesdropping lies with the magistrate's statutory discretion to direct that periodic reports be filed "showing what progress has been made toward achievement of the authorized objective and the need for continued interception." Thus if the progress report reveals the unexplained absence of incriminating calls, probable cause may be lacking for continued eavesdropping; this, of course, depends on the facts of each case. Alternatively, if the report indicates that the investigative objective has been attained, the need for surveillance may no longer be present (here, however, flexibility is once again in order as investigative goals may legitimately change or broaden during the course of surveillance).

Yet, while Title III's progress report provision is well intended, it has generally failed to promote adequate judicial supervision. This failure is attributable to its optional nature and narrow perspective. Many courts do not require progress reports, and those that do often do not receive enough information to effect proper supervision. Moreover, the progress reports are not always carefully reviewed.

For this reason, the nature of Title III's progress report provision should be changed. Most importantly, the concept should be made mandatory, requiring either weekly or bi-weekly reports. Next, their present scope should be expanded to include a report on minimization efforts and evidence of new crimes. Given the complexity of the minimization and retroactive-prospective amendment process, such reports would serve to facilitate compliance. Finally, the reviewing magistrate should be directed to suspend or terminate surveillance if the reports are deficient, evince serious procedural irregularities, or indicate that the legal basis for continued surveillance no longer exists. Such an amendment would promote close judicial supervision and ultimately serve to decrease the risk of electronic surveillance extending beyond its legitimate scope.

4. Preserving the Sanctity of the Tapes

Prior to the passage of Title III, numerous fears were expressed that taperecordings were too vulnerable to tampering to be admitted into evidence. Nevertheless, because of technological barriers, susceptibility to detection, and the availability of far easier ways by which to "frame" a defendant, these fears were generally regarded as unrealistic. Even so, Congress sought to preserve evidentiary integrity by requiring

that, "immediately upon...expiration...of the order or extensions thereof," all tapes must be brought to the issuing magistrate and "sealed under his directions." Further, the statute provides that the presence of this seal, "or a satisfactory explanation for the absence thereof," is a prerequisite to admissibility.

With some exceptions, this provision has only been loosely applied in the courts. The adverse consequences, however have been negligible, for though the judiciary may be faulted for ignoring a statutory directive, the sealing rule presently serves little purpose. In reality, there is nothing sacrosanct about a "seal." Oftentimes, it is merely a piece of tape that is placed around the container in which the taperecording is stored. The tape used to effect the so-called seal may range from simple "scotch" tape to stronger cloth, adhesive-backed tapes. Regardless of which type is used, the tape usually contains a written notation indicating the sealing date and the sealing officer's signature. Together however, the tape and written notations do little to protect the taperecordings' integrity. A forger would have a far easier time removing the tape than he would effecting a successful forgery of the taperecording. Moreover, even if the so-called seal delivered some magical protection to the taperecording, present Title III procedures do not advance this end, as the seal need not be secured until the eavesdropping warrant or extensions thereof have expired. Thus, at least theoretically, ample opportunity exists to tamper with the taperecording before the sealing requirement is even triggered.

Fortunately, allegations of tampering have never become a serious Title III problem. Indeed, this probably explains the judiciary's

reluctance to enforce the current sealing rules strictly. And as the seal is of limited prophylactic value, absent dramatic technological advances in forgery techniques, the formal sealing requirement could be eliminated altogether - especially since the prosecution must still establish the accuracy of each taperecording prior to admissibility. Nevertheless, if sealing is to remain a statutory requirement, the present procedure should be modified to narrow the pre-sealing time period in which opportunity presently exists for forgery to be attempted. My suggestion is that the completed taperecordings be delivered for sealing and storage to the reviewing magistrate within 72 hours of completion. While this would entail frequent trips to the courthouse and administrative burdens for judiciary officials it would be a realistic way to ensure the integrity of each taperecording. The 72 hour figure is suggested because investigators need sufficient time in which to make duplicate recordings (a process requiring only a few minutes for each taperecording, but which often consumes much more time because of transportation, manpower, and administrative difficulties). Finally, failure to comply should not automatically result in exclusion. So long as the taperecording accurately depicts the events in question, suppression should be reserved for situations involving repeated unexcusable delays.

5. Emergency Searches

The authors of Title III recognized that, on occasion, exigent circumstances would warrant electronic surveillance before an eavesdropping warrant could be obtained. Accordingly, warrantless emergency searches were authorized for situations involving national security interests or

the "conspiratorial activities characteristic of organized crime." Such searches are permissible, however only if all statutory requirements could have been met had time constraints not intervened, and provided that, within 48 hours of interception, an application is filed seeking retroactive approval for the eavesdropping.

Nevertheless, while a statutory emergency search procedure is clearly necessary, the present provision is simultaneously ambiguous, unduly narrow, and unnecessarily broad. It is ambiguous because the statute does not define the term organized crime. It is unduly narrow because the provision does not extend to life threatening circumstances not involving national security or organized crime. Moreover, there are often other exigencies involving the need for warrantless surveillance. For example, a vehicle containing a hidden microphone device may cross jurisdictional lines, thereby technically suspending or terminating authorization to eavesdrop. Obviously, under such circumstances, monitoring should be allowed to continue. Finally, the law is unnecessarily broad because there is no reason not to require oral notice to a judge before initiation of surveillance. As presently constituted, if an emergency search is unsuccessful, neither the judiciary nor the intercepted parties would necessarily be advised since no retroactive warrant need be filed. Moreover, given the considerable time usually required to initiate eavesdropping, there is usually no reason why oral judicial approval could not be obtained in advance.

Since enactment, Title III's emergency procedures have rarely been employed. Because this may reflect inadequacies in the present law, the statute should be amended to rectify prevailing deficiencies.

Both law enforcement and civil libertarian interests would benefit as a result.

6. Standards of Review and Suppression for

Title III Violations

Passage of Title III was based upon a system of statutory controls which, with proper judicial enforcement, were designed to preserve Fourth Amendment rights. As much of my summary today indicates, however, statutory protections have often not been effectively implemented by the courts. To some extent, specific amendments can rectify this situation for future litigants, but such measures, standing alone, may be insufficient; historically, a result-oriented judiciary has demonstrated an inclination to gloss over specific statutory language or legislative history when the need to do so was perceived, and this tendency can be expected to continue when a reformed Title III is subject to interpretation. While such a judicial response cannot be absolutely controlled, it may be strongly discouraged by an explicit Congressional directive that, given the importance of the principles at stake, Title III is to be / strictly enforced in the courts.

I should caution, however, that a statement of this kind should not be misinterpreted to the other extreme. It does not mean, for example, that every statutory violation merits the suppression of evidence; quite clearly, harmless errors -- those which are neither intentional nor "affect... substantial rights" -- should not warrant this extreme sanction. Rather, it means that claims of misconduct must be evaluated honestly and rigorously in light of the important policies Congress sought to advance in passing the statute.

Finally, because the proposals I have advanced today would further complicate an already complex statutory process, less reliance should be placed on suppression for procedural errors. Presently, there is something anomalous about a society which seemingly demands perfection from few other than its law enforcement officials. In reality, the adage "nobody's perfect" applies to judges, prosecutors, and police officers as well as to everyone else; mistakes are an inevitable aspect of human existence. Thus, as a general principle, it plainly makes no sense automatically to exclude evidence -- and possibly the fruits of an entire investigation -- merely because someone has erred. And, in the context of Title III, especially once reformed, it makes even less sense to do so. Instead, the focus should be on objective reasonableness and subjective good faith. More specifically, error should not occasion suppression so long as reasonably trained law enforcement officials have made good faith efforts to comply with the law.

This standard, standing alone, is a sufficient and sensible deterrent to official misconduct. Moreover, it can (and should) be reinforced through aggressive enforcement of Title III's criminal and civil sanctions which have thus far largely been ignored. Of course, adoption of this standard, at least insofar as eavesdropping errors violative of the Fourth Amendment are concerned, is contingent on Supreme Court modification of the exclusionary rule in its present form. This issue will hopefully be addressed by the Court shortly. Regardless of its outcome, however, the standard I have articulated will retain vitality for purely statutory violations of nonconstitutional dimension. Hence, the opportunity exists to add significant statutory protection without curtailing effective law enforcement.

CONCLUSION

Title III has provided law enforcement with an effective and constitutional means to achieve organized crime control. Years of experience under the statute have brought to light areas in which its original purpose must be restored as well as numerous improvements that are in order. Nevertheless, in considering reform, Congress should not undo the delicate balance between effective law enforcement and Fourth Amendment rights that was attained under the original legislative design. Indeed, only continued such equilibrium is consistent with the Fourth Amendment's intention to afford protection solely against "unreasonable searches and seizures."

Mr. KASTENMEIER. One of the questions that has occurred to us is that the several sections of Federal law which either prohibit or limit interception of nonoral communications, people have different views about. I am talking about title III and also the Foreign Intelligence Surveillance Act, section 605, the Communications Act.

Assume for the purpose of discussion we wish to clarify this question by merely using the definition of electronic surveillance or contents or wire communication from the Foreign Intelligence Surveillance Act and applying them to title III. That is to clearly prohibit interception without court orders of nonoral communications. What policy questions should we address?

Professor Schwartz, would you like to answer that? Would the expansion of the definition of electronic surveillance cause problems? Would it have the unintended consequence of authorizing law enforcement officers to conduct the search for a general electronic search?

Mr. SCHWARTZ. I don't know if it would encourage them to do that, but it would certainly permit that.

I think what Mr. Carr said at the beginning is crucial. Title III is not a statute to stop electronic surveillance. It is a statute to permit it and it is a statute that was precipitated by a felt need to use electronic surveillance for law enforcement.

Some of us may have disagreed with the weight of that felt need, whether it was, indeed, a great need, but the fact remains that that was its purpose. I think the three of us would tend to agree with that, although perhaps not.

There is no sign at the moment that there is any great need for law enforcement to intercept computer communications or any of these other communications that are not covered. The consequence, therefore, is that you would be taking a statute designed for one purpose, which is to deal with wiretappings, that was the purpose of the statute, and simply importing into it a very different consideration.

Now, the FISA statute does contain a broader range. I think it is because the FISA statute probably was intended among other things, to include videotaping and things like that which were then in the air, no pun intended. There was, I think, some evidence that that had been done in a national security prosecution and I think there was also a feeling that "let's make it as comprehensive as possible" because we are really not talking about law enforcement; we are talking about intelligence.

It seems to me that the consequence of putting it in would be to indicate that it is OK to do that for law enforcement when there is no great need for it. And I would particularly stress my concern about this being made available to State officials.

I don't think the record of State wiretapping is very good. I think the Wiretap Commission reported that the judicial protections were often ignored.

The problems raised by Mr. Goldsmith and Mr. Carr on the Federal level, which are inherent in the statute, are compounded many, many times by simply lax application of the statute. There are some really horrible examples if you read the testimony of the Wiretap Commission of judges say, in effect, well, if the DA, whom I know, puts it in front of me, then I will sign it.

Of course, you were on the Commission and you were there for some of that testimony, Mr. [redacted]. So I think that it is not a good idea. I think this is a hard problem and I think it is a problem that should be faced directly as a special problem of how we deal with the interception and invasions of privacy by largely private people of certain kinds of important communications.

Mr. KASTENMEIER. Well, I addressed the question to you because you did deal with more than title III. But I am wondering whether in terms of new technology particularly and the applicability of old statutes and new technology, we need not look at all these acts together and that there be some consistency and coherence about them, irrespective of the fact that they are intended to achieve other purposes.

Mr. SCHWARTZ. Well, certainly I can't quarrel with that goal of coherence. I do think, however, if you are going to look at the different statutes, then, in effect, you are engaging in the amending process or looking to the amending process. And if you are doing that, it seems to me one ought to focus on the specific problems. It may well be that the Intelligence Act really should not have that broad a definition because it should not reach computer communications.

The thing about title III that is different from the Intelligence Act is that it is a criminal statute. That would be the bite if you are trying to reach inappropriate private interceptions.

The FISA Act is an act that permits the Government to do something. There you may want a broader definition and there may be no harm; I am not sure. You certainly don't have the State problem that I alluded to. But it seems if you are going to engage in the amending process, then it seems to me you ought to address what seemed to me, and from conversations with some people in the computer industry, to be some very unique and troublesome problems. Someone else can address those better than I can, obviously, but it seems that those problems should be addressed separately.

Mr. KASTENMEIER. Both Mr. Carr and Mr. Goldsmith indicate there ought to be, I gather, changes in title III of some consequence, changes perhaps for other purposes.

As Mr. Carr points out at the outset, title III, the legislative history of title III, does not give us any reason to expect that it was the last word, that we should think that it was perfectly written. And we seem to have, additionally at this point in time, the incentive of what is covered and what is not covered in terms of its conceptual exclusion.

Would you say, Mr. Carr, that if one rewrote title III we ought to use it rather than as an authorizing statute as a statute limiting its utility?

Mr. CARR. I think in theory that is how title III is presently constructed. I say in theory because it begins with an absolute prohibition of all forms of electronic surveillance or oral interception. I think that is not the precise question.

The question is, how can we make the authority more limited than we do now? And I think Mr. Goldsmith, as I was sitting here, I think there are 8 or 10 points in the statute that all three of us I think would agree should be amended to accomplish that result. In other words, to limit the circumstance in which title III can be

used. A title exhaustion requirement, a more expansive naming and notice requirement, more effective judicial control.

I know I am repeating, but I am doing it to emphasize the agreement that I think the three of us have through mandatory periodic reports, more effective implementation and minimization.

I think that these kinds of things and one other point—and I underscore this—would be to require a statement in the application of what the objective of the investigation is. That is a key phrase in title III, because once the authorized objective has been accomplished, the surveillance is to stop.

It is a termination provision but nowhere in the statute does it require the authorities to state at the outset what that objective is. Therefore, it is something that is self-defined, not expressed, never judicially ratified. So I think it would be crucial to require that as part of the application process. I believe Professor Goldsmith would agree with that.

So, to answer your question, Representative Kastenmeier, I think that title III will remain a statute intended to permit law enforcement surveillance. I don't think we can get away from that. I think it can be improved to limit the extent and circumstances in which that surveillance occurs.

It is going to take one more moment. There is one other area of serious ambiguity in the present statute, and Professor Schwartz mentioned the Wick situation, and that is the question of whether recording by a participant, simple recording, not transmitting, but simple recording by a participant to the conversation, whether or not that is covered by the definition of interception in the present title III.

I think that it would be appropriate to amend the statute to state simply, "recording of a conversation by a participant is an interception," and that would resolve that ambiguity and it would resolve it in favor of privacy interests as opposed to either self-help desires on the part of private citizens or law enforcement interests.

Mr. KASTENMEIER. I think at this time I should yield to my colleague from Massachusetts who is only a slenderized version of his former self.

Mr. FRANK. Thank you, Mr. Chairman, relatively so. I appreciate your having this hearing. I think these are very important, and it is useful for us to be able to talk about them without a specific crisis.

I also benefited from the specific expertise of the witnesses, and I will be going back over that. But I would like also to focus on a couple of general questions that I think many of the specifics on which there are agreement on things that I think we ought to press on, and my questions really do deal with the general tradeoff that we have to make when we talk about authorizing wiretapping.

Professor Schwartz indicated a little more skepticism about it.

The question I am going to ask you is obviously not subject to great quantification, I understand that, but I think in the opinion of all three as to how much abuse does go on. There is obviously a question about how essential wiretapping is for the legitimate law enforcement purposes. We can argue about whether or not it is legitimate if the judge says "OK," and you really are restricting it to

the purposes you are supposed to, but there are obviously potentials for abuse.

I would be interested in the experience of each of you. To what extent do we have a problem that people are getting listened to by overzealous prosecutors in situations where judges rubber stamp? How much of that is happening, and are there abuses that are now a problem because people are listening to other people when they shouldn't be, and if there are, is there any pattern of that stuff being used improperly? Have we got cases where people are hearing things they shouldn't hear, and have been using it in ways that are improper?

I would be interested in all of your views on that.

Mr. GOLDSMITH. Maybe I could address myself to that initially. I think in the context of any statute, substantive or procedural statute, there is going to be the potential for abuse, and I think likewise we can say that there are always going to be abuses of sorts.

The purpose of legislation, however, should be to craft a statute that minimizes the extent of possible abuse. One of the reasons that there may have been abuses under title III in the past—

Mr. FRANK. We don't have a lot of time. I agree with you that those are the purposes of the statute. One of the things I need to know is people's general opinion on whether there are or are not abuses. I assure you that if you say there are abuses, I will not be for the repeal of title III. I understand all that about what we should be doing and what we shouldn't be doing.

Mr. GOLDSMITH. I think that the nature of the abuses has frankly been very minimal. I have seen Federal and State prosecutors instruct their monitors as to how the surveillance is going to be done. These meetings take hours. I have seen Federal and State prosecutors review the daily surveillance logs of what has been obtained the day before and go back to the monitors and say that you shouldn't have taken this or you should have taken this. The nature of the supervision ironically is a lot tighter from the prosecutorial level than it is from the judicial level.

Mr. FRANK. I appreciate that. And again, I was not presupposing that there was a lot of abuse. Might not some of that excessive care, which I am glad they are taking, be lessened if we adopted good-faith exception to the exclusionary rule? To what extent is all of that very very patient and laborious instruction—might that be vitiated if there was a good-faith exception?

Mr. GOLDSMITH. I think that if anything, it would advance it because if you have a good-faith exception—

Mr. FRANK. Well, the more they know, the less likely they are to take advantage of a good-faith exception. If people didn't know that much, they would be more likely to be making mistakes in good faith.

Mr. GOLDSMITH. I would say that good faith has not been achieved unless certain minimal standards have been met. If law enforcement has not been properly trained and instructed in general on how the particular tap is to be conducted, then you can't say you have been acting in good faith.

Mr. FRANK. Then you might say that the kind of effort you have seen a large number of prosecutors engage in if you were going to have a good-faith exception might be a prerequisite for qualifying.

Mr. GOLDSMITH. Yes, in other words, there is an objective component to good faith.

Mr. FRANK. I always have problems with objective good faith. I agree with you about this.

Mr. SCHWARTZ. With all due respect, I think that is nonsense.

Mr. FRANK. What part of it?

Mr. SCHWARTZ. What my colleague, Mr. Goldsmith, said. I think judges are very reluctant to exclude evidence. That is the fundamental problem.

Mr. FRANK. He said that he thought the safeguards in fact came off in the prosecutors and the judges.

Mr. SCHWARTZ. But the only time the good-faith defense would have any meaning is when the judge excludes the evidence and judges don't want to exclude relevant evidence. That is the fundamental problem. You have relevant evidence that somebody has had his hand in the till or something or is selling narcotics. That might be a good thing or a bad thing to exclude, but if you are going to have the exclusionary rule, have it because judges don't want to exclude evidence, and they will buy anything in the world that consists of good faith, including stupidity.

Mr. FRANK. I appreciate that, and I am the guilty party here in having diverted everybody from what I was interested in. I appreciate that, but what about the general sense about the degree, if we have literal abuse, are the Federal people better than the State?

In terms now of people listening when they shouldn't be and hearing things they shouldn't and maybe misusing what they have heard?

Mr. SCHWARTZ. That is an almost impossible question to answer simply because we don't know what happens. We only see what surfaces in court, and we do know, depending on the definition of what you are talking about as an abuse.

For example, on the State level, the Wire Tapping Commission testimony, and Mr. Kastenmeier was there and may or may not bear me out on this, on the State level the procedures are utterly worthless. With rare exceptions, judges insist on almost nothing. What does that mean, that people are being overheard who shouldn't be overheard? Probably.

Mr. FRANK. Well, is it your impression? I understand that it is a difficult question, but I think we need to take a cut at it if I am going to vote on these things. Are prosecutors at the State level inclined toward abuse, some are, some aren't? Are there patterns where they do too much of this or are they constrained by the number of men they are going to tie up?

Mr. SCHWARTZ. Some prosecutors are and some aren't, but your basic problem is not the prosecutor; it is the policeman. It is the policeman who listened in in California on attorney-client conversations and kept a separate set of cassettes. Some he turned in to the court and some he kept for himself.

Mr. FRANK. Is there a pattern of police doing this without prosecutorial OK? I don't follow that.

Mr. SCHWARTZ. Normally, when that will happen, the prosecutor hears about it privately if he is the prosecutor, like I assume Mr. Goldsmith is, and some others, he would say "Don't do that again."

if it gets to court, the prosecutor will fight as hard as he can to keep it admissible.

Mr. FRANK. But in terms of the statute, I assume that a law enforcement agent without a prosecutor's OK, is there any ability under the statute for the cop to just do it on his or her own without the prosecutor going through the procedure?

Mr. SCHWARTZ. Not under the statute, no.

Mr. FRANK. Well, I understand that if people are going to do that—

Mr. SCHWARTZ. But under the statute I am saying that police who get a warrant to go and put on a tap will ignore the minimization procedures and listen to everything under the Sun. The prosecutor will say to him, "Don't," and they do.

Mr. GOLDSMITH. The truth is that oftentimes what is not pertinent is so boring that they are going to shut it off. They are there for 24 hours a day and they are told to minimize, and aside from the fact that they have been given the instructions, oftentimes it is so boring that they don't want to listen to it. Beyond that, the type of example that Professor Schwartz has just given us, that individual who kept his own set of tapes should have been prosecuted. That was a crime. He, in fact, should have been prosecuted.

Mr. SCHWARTZ. And when was the last time a policeman was prosecuted for any kind of abuse like that?

Mr. GOLDSMITH. Agreed. Those kinds of situations should be handled by criminal prosecutions, as well as civil suits. What that policeman did, frankly, was an outrage.

Mr. FRANK. Did the policeman in this case do it on his own, or was this a prosecutorial and judiciary authorized thing and he just went too far?

Mr. GOLDSMITH. I don't know the facts of that case. I only know what Professor Schwartz has just given us, but that hypothetical is an example—

Mr. FRANK. I gather it is not hypothetical.

Mr. SCHWARTZ. Oh, no, I am reading from the Wiretap Commission studies. It is a marvelous document. There is a statement by the Commission on findings which says one thing on the majority, and then you have volumes of testimony which refute it totally, and I got this information from the Wiretap Commission hearings including a New Jersey policeman admitting that if someone were overheard talking to his lawyer, the police would listen in and any instruction to minimize would be ignored.

Mr. FRANK. I understand that, and I realize it is a difficult question, but I think we all have opinions, those of you particularly who are specialists, as to whether or not there is a tendency to ignore or not. I think it is a useful law enforcement tool, but that could be curtailed by the extent of abuse.

Mr. Carr?

Mr. CARR. I was about to say that I have found since an abandoning the law, a teaching career, that wearing a black robe allows me to interrupt lawyers on occasion. I was about to interrupt, and I wish I had my robe.

My sense is that the extent of abuse, and defining that very broadly, unnecessary electronic surveillance or surveillance that occurs, though court ordered, occurs outside the restrictions of the

statute is slight at the Federal level. Given the cost and the incredible internal control that is exercised——

Mr. FRANK. Is that basically prosecutorial self control?

Mr. CARR. I think it is controlled within the agency itself. One thing that I have learned since becoming a magistrate and not being a professor is that the FBI is an incredibly regimented and hierarchial institution.

Mr. FRANK. Don't professors know that? I think most of them know that.

Mr. CARR. One professor didn't know that, and I think there is an amazing quantity and quality of internal control within the Bureau. I don't know, because I haven't had exposure to DEA and some other agencies and certainly at the level of assistant U.S. attorneys and strike force people have considerable control and concern about the exclusionary role.

At least the second point, I would disagree vehemently with the suggestion that whatever the Supreme Court does with *Map v. Ohio* ought to be mimicked in title III. Title III has its own somewhat unique exclusionary rule in section 2515. At least leave it alone if you don't tighten it up.

Mr. FRANK. Your feeling is that part of the reason we have good results at the Federal level is the effect of the exclusionary rule?

Mr. CARR. Absolutely. I have no doubt about that at all because particularly when you have a protracted surveillance operation, if you stumble coming in the door, the whole thing is going to go out the window. And if you had a good faith exception, that interregnum effect would not exist, and I think it is crucial.

But I do think that there is an enormous opportunity for abuse, and I think actual abuse, given the total lack of regulation of consent surveillance, both by private parties and by law enforcement officers.

There was a question about whether a police officer has been prosecuted. I believe 10 years ago in New York City, the special investigation unit which had access to wiretapping devices used them unlawfully. Some 60 police officers were prosecuted.

Mr. SCHWARTZ. That was corruption. That is not wiretap violations.

Mr. CARR. Yes, but it began, I understand, with unlawful use of——

Mr. FRANK. The police officers in question were using these things?

Mr. CARR. Because, No. 1, they had access to them. They are part of the equipment that is available and frequently not without internal control, and, second, there is no regulation. You can engage in surreptitious consent surveillance, and I shouldn't use the word "surreptitious," consent surveillance without any prior regulation. Again, although in the *United States v. White*, the Supreme Court held that prior warrant is not required.

I would commend to the committee a reading of Justice Harlan's dissent because I think he lays out the issues and concerns.

Mr. FRANK. Your responsibility is primarily Federal. Is it your sense then that the States, or some of them, may not be as good as the Federal Government is in living up to these things, or you just do not have the evidence one way or the other?

Mr. CARR. I would agree with Professor Schwartz that the States' misuse of court-ordered surveillance and surveillance devices is potentially far greater because you have the local county prosecutor who is the person who is in charge. It has been filtered down all the way to the local level.

By way of background, it is my understanding that the reason we have authorization for State surveillance in the first instance is that in 1968 a Federal wiretap statute could not be adopted unless the district attorney's office in Manhattan had the opportunity to engage in its wiretapping, it having been in the forefront. If you let Manhattan do it, you have to let South Dakota, Colorado, and Hawaii do it.

Consequently, we have this very broad authority at the State level which to me is of very much greater concern about potential abuse than the Federal level.

Mr. FRANK. Mr. Goldsmith.

Mr. GOLDSMITH. Incidentally, as to consent surveillance, I am very much in favor of permitting interception without court order when one party consents to it, characterizing this as consensual surveillance is really a misnomer because the subject of the investigation is not consenting to it.

Mr. FRANK. It sounds better than conceptual tapping. Conceptual tapping seemed to be mildly erotic.

Mr. SCHWARTZ. I said consensual tapping.

Mr. FRANK. It sounds like more fun than what we usually do.

Mr. GOLDSMITH. Such surveillance has been referred to as an intrusion on trust. I think the flip side of the intrusion on trust is giving the person who is the target of the investigation, in essence, license to lie. If the tape is excluded, that person relies upon the faulty memory of the person who was conducting the investigation.

Moreover, oftentimes in law enforcement situations, you need to equip an undercover agent with a monitoring device because he, in fact, is in a very dangerous situation. You want to have your people outside to protect the safety of the person inside. They need to know what is going on.

Mr. FRANK. It didn't work on the "Hill Street Blues" last week, though.

Mr. GOLDSMITH. That is right, it didn't.

Mr. FRANK. But I understand the point.

I don't want to overdo, Mr. Chairman. I appreciate it, gentlemen, but I think we do have other members here, and we may continue this later, but I am going over my time. It is not your fault.

Mr. KASTENMEIER. We do have other witnesses, and I do want to thank our three witnesses this morning, Professor Schwartz, Professor Goldsmith, and Magistrate Carr, for their appearance before this committee.

Mr. CARR. Thank you.

Mr. GOLDSMITH. Mr. Chairman, might I request the Commission to file a brief statement on the question of consensual electronic surveillance.

Mr. KASTENMEIER. We would be very pleased to receive the statement, and, without objection, it will be made a part of the record.

Mr. GOLDSMITH. Thank you very much.

[The information follows:]

A Statement for the Reform of Federal Eavesdropping Legislation

By Professor Michael Goldsmith

I would like to thank the Judiciary Committee of the United States House of Representatives for inviting me to express my views on the subject of electronic surveillance. Presently, I am an assistant professor, on leave from Vanderbilt Law School, serving as Counsel to the New York State Organized Crime Task Force. My testimony today, however, represents my views alone rather than those of any institution.

My understanding is that the Committee would like me further to develop aspects of an article that I recently authored entitled The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance, 74 J. Crim. L. & Criminology 1 (1983). More specifically, I have been asked to provide suggestions for reforming Title III, the federal law which governs the use of nonconsensual electronic surveillance in this country. Given the thesis of my article -- that the Supreme Court has, in effect, rewritten Title III through a series of decisions which deviated from the Court's original guidelines for the enactment of a constitutional eavesdropping statute -- legislative review of this issue is certainly appropriate. Significantly, previous efforts at legislative reform, such as S. 1630 introduced before the 97th Congress, sought to effect significant improvements, but failed to realize the extent to which Title III has been modified by decisional law.¹

Accordingly, this statement will set forth a series of proposals for reform of Title III. For the most part, these proposals were either explicitly or implicitly made in my article. Since I cannot hope to duplicate in this statement the detailed analysis contained in a 171

page article, emphasis of key points rather than comprehensiveness of analysis will be my primary goal. For more detailed analysis, citations to my article or to other sources have been provided. Finally, please note that, as I have had the benefit of both additional experience and collegial commentary since the article was published, some of the proposals are modifications of those which I originally made.

I have organized my remarks to emphasize the six areas I believe are most deserving of legislative attention: 1. Standing to Contest Title III Violations; 2. The Need to Exhaust Investigative Alternatives; 3. Controlling the Duration and Scope of Interception; 4. Preserving the Sanctity of the Tapes; 5. Emergency Searches; and 6. Standards of Review and Suppression for Title III Violations. My discussion of each area will usually include both civil libertarian and law enforcement concerns, for each perspective must be meaningfully considered if Title III is to be properly revised. As such, law enforcement supporters must acknowledge the legitimate concerns of those who fear the intrusiveness of an electronic search; likewise, civil libertarians must concede that court authorized electronic surveillance is a reasonable way, indeed, the only way, to combat effectively the severe social and economic consequences wrought upon our society by organized criminal groups. Title III is already an extraordinarily complex piece of legislation that the National Wiretapping Commission recognized as having afforded law enforcement with a vital investigative tool while simultaneously preserving Fourth Amendment rights.² In considering reform, great care must be exercised to avoid imposing requirements that would make resort to electronic surveillance unduly burdensome or effect

the suppression of evidence for every sort of statutory violation. Constitutional rights are, in fact, advanced through a system that discourages police misconduct by providing a reasonable way to achieve investigative goals legitimately.³ It is with this sense of balanced perspective that I urge the Committee to evaluate the proposals which follow.

1. Standing to Contest Title III Violations

By legislative design, standing to contest alleged Title III violations is a prerequisite to the availability of the statute's evidentiary suppression remedy that is intended to deter misconduct.⁴ In this regard, Title III appears to grant claimants the benefit of a liberal standing rule by defining the term "aggrieved person" as "a person who was a party to any intercepted wire or oral conversation or a person against whom the interception was directed" (emphasis added).⁵ Yet, although this broad language seems to confer so-called target standing upon potential litigants, by authorizing anyone "against whom the interception was directed" to raise a suppression claim, the Supreme Court has effectively restricted Title III standing to intercepted parties or anyone whose telephone or facility is the subject of surveillance. Unfortunately, this effect was achieved as a result of some dicta, rendered in Alderman v. United States⁶ without the point ever having been briefed,⁷ suggesting that Title III standing was quite limited in scope.⁸ The Alderman dicta, however, was inconsistent with the statutory definition of "aggrieved person", and ignored a substantial body of legislative history which seemed to indicate that target standing was intended by Title III's authors.⁹ Admittedly, the Supreme Court has recently rejected target standing in the constitutional law context,¹⁰

but that ruling obviously has nothing to do with the legislative intent underlying Title III at the time of its enactment.

As a policy matter, it should be apparent that target standing is the only practice which squares directly with Title III's goal of deterring illegal electronic intrusions. Simply put, absent target standing, prosecutors and police are relatively free to tolerate or even encourage misconduct in those situations in which the intercepted party (or facility) does not involve the target of the investigation.¹¹ Under such circumstances, law enforcement may have incentive to violate the rights of suspected lower echelon criminals -- secure in the knowledge that higher echelon investigative targets will not be in a position to assert a Title III claim. While such conduct by law enforcement officials would potentially expose them to statutory criminal and civil liability,¹² Title III's criminal and civil provisions have rarely been utilized. Fortunately, no evidence has emerged of such prosecutorial misconduct, but, to avoid this occurrence, the statute should be specifically amended to provide for target standing.

Any such amendment, however, should give ample consideration to law enforcement's legitimate concern that blanket target standing may have disproportionate consequences if a violation which directly affects a few individuals is permitted to taint subsequent investigations as well.¹³ Not all violations pose such a risk, but the potential nevertheless exists. This risk, however, can be minimized by requiring law enforcement authorities to specify their investigative objectives and targets in the eavesdropping application. Arguably, the statute already implicitly requires a statement of objectives in order for a reviewing

magistrate to assess the investigative need for surveillance and the duration for which eavesdropping is to be authorized (concepts which are discussed in sections 2 and 3 below), but many applications make no specific reference to investigative objectives. Adoption of such a requirement would allow the scope of standing to be determined directly by reference to the eavesdropping application. This requirement would also have the advantage of motivating law enforcement officials to state their investigative goals conservatively, thereby often narrowing the scope and duration of surveillance. Any problems involving subterfuge omissions could be handled by piercing the statement of objectives and targets, with standing being extended to persons for whom there was reasonable cause to believe involvement in the activity under investigation.¹⁴ Excessive taint should not occur for, as with inaccuracies in traditional search warrant affidavits, the burden of establishing an intentional or reckless misstatement would lie with the defendant.¹⁵ Finally, traditional attenuation principles would still operate to limit undue consequences of the suppression sanction.¹⁶

Finally, there is an aspect of standing in the grand jury context that merits reform. In Gelbard v. United States,¹⁷ the Supreme Court correctly interpreted Title III to provide a just cause defense for grand jury witnesses who seek to avoid the contempt sanction by arguing that their refusal to testify is predicated upon questioning derived from illegal electronic surveillance.¹⁸ Gelbard, however, failed to provide guidance concerning the extent to which court authorized surveillance must be disclosed to the witness during the course of resolving such claims, and lower courts have since been divided.¹⁹ While

the language of Title III presently seems to mandate limited disclosure to the witness.²⁰ I believe that no such access should be allowed. Given the relatively limited extent of present disclosure, little is accomplished towards protecting the witness' constitutional rights that could not adequately be achieved by in camera judicial review. Moreover, few recalcitrant witnesses are concerned with vindicating their Fourth Amendment rights. Historically, most such witnesses (other than victims of crime whose recalcitrance typically reflects safety considerations)²¹ are anxious for purely tactical reasons to learn whether their questioning is derived from electronic surveillance.²² If so, the witness will usually attempt to tailor his testimony carefully to what he believes the prosecutor already knows; if not, the witness often realizes that he has, in effect, a license to lie. In camera judicial review, with the witness merely being advised that his questioning is not based upon illegal electronic surveillance, will avoid this result.

Admittedly, since this proposal is based upon the limited disclosure presently authorized by Title III, some might argue that my premise would be undercut if the statute were amended to provide for complete disclosure to grand jury witnesses. Such an approach, however, would inevitably embroil grand jury inquiries in lengthy suppression hearings, a consequence fundamentally at odds with efficiency considerations that have long governed grand jury procedure in our society.²³

2. The Need to Exhaust Investigative Alternatives

In providing guidelines towards the enactment of a constitutional eavesdropping statute, the Supreme Court strongly suggested that resort to electronic surveillance should not be permitted when less drastic

investigative alternatives are available.²⁴ This viewpoint was incorporated into the statute by the requirement that each surveillance application include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."²⁵ While Congress intended this requirement to be applied in a common sense manner, so that law enforcement authorities should not feel constrained to expend time and resources on obviously futile investigative efforts,²⁶ the statute plainly calls for a "full and complete statement" from which the reviewing magistrate can realistically assess the need for surveillance. Oftentimes, however, this requirement has been deemed satisfied by boilerplate assertions that investigative alternatives have been exhausted. Relatively few opinions have carefully analyzed whether the exhaustion statement is full and complete, much less whether it is based on substance.²⁷ A probable consequence is that electronic surveillance occasionally has been approved when less drastic means may have sufficed.²⁸

The present situation can be ameliorated by an amendment requiring that the exhaustion statement contain, in effect, an investigative checklist (as set forth in the revised statute) of every alternative reasonably available and an explanation of its inutility.²⁹ This amendment should likewise be interpreted in a common sense fashion, as its purpose is not to encourage futility (nor should suppression necessarily follow because a particular technique was not used.) Rather, it would serve to ensure that the judiciary has been provided with an adequate factual basis to evaluate the need for an intrusive electronic search. Furthermore, given the need to supply such a statement, it is likely that law enforcement will file fewer unnecessary applications.

Finally, the requirement of a statement of objectives (see section 1) should be regarded as a corollary to this improved exhaustion statement. Indeed, absent a statement of objectives, neither investigative need nor the proper duration for eavesdropping authorization can be realistically appraised. For this reason, specificity of objectives is already an implicitly required component of the exhaustion statement. Nevertheless, since many eavesdropping applications have not been sufficiently specific in this regard, an explicit requirement to this effect should be adopted.

3. Controlling the Duration and Scope of Interception

A. Surveillance of unknown parties

A major point of controversy in the Congressional debate over electronic surveillance concerned the number of persons potentially subject to eavesdropping.³⁰ In an effort to limit the scope of interception, Title III seemingly limited surveillance to identified persons for whom there was probable cause to believe participation in specified discussions of criminality.³¹ While the statute clearly contemplated such persons inevitably being overheard in conversations with unknown individuals, it apparently did not countenance long term interception of discussions exclusively involving unidentified parties. Thus, just as traditional search warrants operate to protect the rights of unknown third persons by requiring the object of the search to be identified, Title III was designed to protect this category of individuals by limiting surveillance to conversations involving at least one identified person.³²

This protective mantle of Title III was undercut by Supreme Court dicta in United States v. Kahn³³ and United States v. Donovan³⁴

suggesting that eavesdropping warrants may authorize surveillance of specified persons "and others as yet unknown."³⁵ The dicta was grounded in the notion that "[t]he Fourth Amendment requires a warrant to describe only 'the place to be searched, and the persons or things to be seized,' not the persons from whom things will be seized,"³⁶ a narrow constitutional construction fundamentally at odds with the well established principle that "the Fourth Amendment protects people, not places."³⁷ Apparently, the Court had failed to consider that specificity of party in an eavesdropping order is necessary to provide unknown third persons with constitutional protection equivalent to that which they are entitled under a traditional search warrant.³⁸ Moreover, even though Title III's legislative history indicates that Congress appreciated the need to protect unknown third parties, and, accordingly, limited the scope of interception to conversations involving at least one known individual,³⁹ the Kahn Court proceeded to suggest that surveillance against exclusively unknown persons was statutorily permissible as well.⁴⁰

To restore the proper protective scope to Title III, an amendment should be adopted restricting eavesdropping to conversations involving at least one identified party. Conversations between unknown persons should not be subject to interception unless probable cause exists that virtually everyone using the designated facility or telephone is doing so for the illicit purpose set forth in the warrant.⁴¹ An exception should also be allowed for the early surveillance period when monitoring agents are in the process of becoming familiar with the voices of their targets;⁴² moreover, provision should be made for anyone intercepted "in plain view" during this period to be expeditiously added to the eavesdropping

warrant. For example, such amendments should be permitted without additional Attorney General approval or the need to exhaust investigative alternatives (Cf. section 3.C below). In this way, the present scope of interception can be substantially narrowed without unduly impeding effective law enforcement.

B. Minimization of nonpertinent conversations

In a further effort to limit the scope of interception, Title III requires that "the authorization to intercept...shall be conducted in such a way as to minimize the interception of [nonpertinent] communications...." (emphasis added).⁴³ Accordingly, monitoring agents are not permitted to intercept conversations not relevant to the target, crime, and conversation specified in the eavesdropping warrant. While perfection obviously cannot be expected--some interception being inevitable as the monitor listens to determine pertinency--minimization was perceived as a reasonable way to discourage eavesdropping not relevant to the court order.⁴⁴ Indeed, when the Supreme Court commented in Kahn on the permissibility of intercepting "others as yet unknown," the minimization requirement was cited as providing an adequate safeguard against sweeping general searches.⁴⁵

Unfortunately, however, the minimization principle has often been given minimal effect. In part, this may be attributed to the courts' willingness to apply judicial minimization guidelines too uncritically; consequently, minimization violations are rarely found (this tendency may be reversible by a Congressional directive calling for strict enforcement; see section 6 below).⁴⁶ But, more fundamentally, by virtue of the Supreme Court's decision in Scott v. United States,⁴⁷

monitoring agents are, in effect, encouraged to seize any conversation whose interception can be justified under existing guidelines -- regardless of whether the conversation is actually nonpertinent.⁴⁹ Scott held that, notwithstanding the monitoring agents' purposeful failure to initiate minimization efforts, no violation has occurred if the resulting seizure is still viewed as objectively reasonable under prevailing minimization guidelines.⁴⁹ Thus, subjective bad faith is not considered in determining whether the minimization requirement has been violated.

From a statutory perspective, Scott was wrongly decided, and, therefore, should be legislatively reversed. The decision disregards the Congressional directive that eavesdropping orders be "conducted in such a way as to minimize interception of [nonpertinent] communications."⁵⁰ Moreover, if subjective good faith is not required when executing an eavesdropping warrant, the statute's broad deterrent purpose is substantially undermined.⁵¹ Indeed, Scott seems to have tolerated conduct which was actually felonious under Title III's criminal sanctions.⁵² Therefore, to reinvigorate the minimization requirement, an amendment should be adopted providing that alleged violations be considered from both an objective and subjective standpoint.

A related problem in the minimization context is the extent of suppression that should be mandated when illegality has occurred. Most courts have limited suppression to the improperly minimized conversations themselves.⁵³ This solution, however, does not sufficiently penalize violators, since law enforcement loses only that to which it was never entitled; moreover, such conversations are often innocent discussions that are not relevant to a criminal prosecution.⁵⁴ Nevertheless, at the

INTENTIONAL

BLANK

other extreme, total suppression would be a disproportionate remedy, as isolated minimization violations should not be allowed to taint an otherwise proper long term investigation. A suitable legislative compromise would be one that establishes a middle ground between these two alternatives. For example, an appropriate accommodation might focus on whether the minimization violations constitute a pattern of illegality. If so, all conversations seized during the course of that pattern should be suppressed (e.g., all calls intercepted on a particular day or by a particular monitor).⁵⁵ Moreover, if multiple patterns -- suggestive of recklessness or intentional misconduct -- occur, total suppression would be in order. This remedy would provide an adequate disincentive against minimization misconduct without unnecessarily jeopardizing an entire investigation.

C. Retroactive and prospective amendments

While Congress was concerned about limiting the scope of eavesdropping, it recognized that monitoring would often expand beyond the crimes specified in the warrant.⁵⁶ By analogy, as officers executing a standard search warrant may properly seize unanticipated evidence that comes into "plain view,"⁵⁷ surveillance monitors may unexpectedly come upon conversations involving criminal activity not described in the court order. Indeed, assuming that proper minimization techniques are being employed, discovery of new crimes is a desirable consequence of electronic surveillance. Therefore, Title III allows evidence of such crimes to be admissible "when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the

provisions of this chapter. Such application shall be made as soon as practicable."⁵⁸ Thus, a statutory plain view procedure has been established providing, in effect, for retroactive amendment of the original eavesdropping warrant once the interception's propriety has been judicially determined. Arguably, this procedure exceeds constitutional demands, as the Fourth Amendment does not require a comparable retroactive amendment "as soon as practicable" for conventional search warrants that result in plain view seizures; instead, the propriety of the seizure awaits determination at the eventual suppression hearing.

Regardless, few courts have enforced Title III's requirement that retroactive approval be sought as soon as practicable.⁵⁹ This tendency, which may be due to the difficulty of determining practicality, could be easily rectified by requiring that, to the extent realized, evidence of new crimes be set forth in periodic progress reports to the magistrate who issued the warrant (see section 3 below). At that time, the judge could rule on the propriety of the interception, but he should also be allowed to defer judgment until the pretrial suppression hearing when the full context of the case can more effectively be presented to him.

The more serious omission in this area has been the judiciary's failure to evaluate critically the admissibility of new crime evidence under traditional Supreme Court guidelines for plain view seizures: 1. whether the initial intrusion was valid; 2. whether the conversation's incriminating character was "immediately apparent;" and 3. whether the discovery was inadvertent.⁶⁰ Together, these guidelines were designed to ensure that law enforcement does not use the plain view concept as a

pretext for effecting general searches. Because this standard may be constitutionally required, its enforcement would be advanced by specific incorporation into the statute. However, as the Supreme Court has suggested that the plain view doctrine may soon be revised,⁶¹ any amendment should await, or be subject to, such modification.

From a law enforcement standpoint, the retroactive amendment requirement has occasioned serious difficulties in some circuits that have interpreted the provision too rigidly. These courts have suppressed evidence by holding that the procedure applies even to statements which happen to pertain both to the crime specified in the warrant and some other offense.⁶² Since, under such circumstances, the intercepted remarks are already within the terms of the eavesdropping warrant, the propriety or scope of the seizure requires no further clarification. By analogy to conventional searches, the situation is equivalent to a seizure by warrant of a suspected homicide weapon which is later (or simultaneously) determined to pertain to a separate robbery incident as well. Since Title III clearly was not intended to require retroactive amendments in such situations, legislative reversal of the offending decisions is in order.

Finally, implicit to Title III is the requirement that a prospective amendment to the eavesdropping order be obtained as soon as there is probable cause that new crimes will be intercepted. This mandate is a consequence of the inadvertence component to the plain view doctrine.⁶³ More specifically, since inadvertence for plain view purposes is defined objectively as the absence of probable cause,⁶⁴ retroactive amendments may be approved only when there was no probable cause to believe that evidence of new crimes would be overheard. Therefore, when

the requisite probable cause exists, a prospective amendment should immediately be obtained as the interception can no longer be justified on traditional plain view grounds.

This process, however, places law enforcement in an intractable dilemma: if a prospective amendment is issued, defense counsel will argue the absence of probable cause; conversely, if no such amendment is obtained, defense counsel will contend that plain view retroactive approval should not be granted because there was probable cause to anticipate the interception of new crime evidence, and, therefore, a prospective amendment should have been sought. Moreover, there are further difficulties for the prosecutor who seeks a prospective amendment. Because the statute does not expressly require such an amendment, there are significant questions concerning which procedural requirements are prerequisites to its issuance. For example, must the Attorney General (or designated Assistant Attorney General) approve such applications in the same manner required for the original eavesdropping application? If so, bureaucratic delay will inevitably preclude timely amendments. Also, must the exhaustion mandate be satisfied as to the new crimes evidence? If so, valuable evidence may be lost by requiring monitors to terminate interception when the conversation turns to new areas of criminality. Finally, may a prospective amendment be obtained when the new crime is not one of those authorized by statute for interception.

Perhaps for these reasons, the courts have largely ignored the prospective amendment concept.⁶⁵ Nevertheless, since the supreme court has recently questioned whether inadvertence is, in fact, a component of the plain view doctrine,⁶⁶ legislative reform should await further judicial clarification. If inadvertence is (ultimately) deemed to have constitutional vitality, a specific statutory procedure should be

provided for addressing these problems. The procedure adopted should be sufficiently accommodating to the difficulties outlined above. Thus, for example, where good faith has been exercised and a prospective amendment obtained, probable cause should be flexibly and reasonably interpreted;⁶⁷ alternatively, perhaps a modified "inevitable discovery" doctrine could resolve the prosecutor's dilemma.⁶⁸ As to Attorney General approval, exhaustion, and non-designated crimes, flexibility should likewise be the key. Under such circumstances, judicial review of probable cause and the nature of the offense is sufficient to safeguard Fourth Amendment rights. Additional protection could be secured by requiring retroactive Attorney General approval within ten days of the prospective amendment's issuance. In this manner, the statute could be brought into constitutional conformity without precluding effective law enforcement.

D. Mandatory progress reports

Since Title III is substantially premised upon close judicial supervision of electronic searches,⁶⁹ a final precaution against improperly expansive eavesdropping lies with the magistrate's statutory discretion to direct that periodic reports be filed "showing what progress has been made toward achievement of the authorized objective and the need for continued interception."⁷⁰ Thus if the progress report reveals the unexplained absence of incriminating calls, probable cause may be lacking for continued eavesdropping; this, of course, depends on the facts of each case. Alternatively, if the report indicates that the investigative objective has been attained, the need for surveillance may no longer be present (here, however, flexibility is once again in order as investigative goals may legitimately change or broaden during the course of surveillance).

Yet, while Title III's progress report provision is well intended, it has generally failed to promote adequate judicial supervision.⁷¹ This failure is attributable to its optional nature and narrow perspective. Many courts do not require progress reports, and those that do often do not receive enough information to effect proper supervision. Moreover, the progress reports are not always carefully reviewed.

For this reason, the nature of Title III's progress report provision should be changed. Most importantly, the concept should be made mandatory, requiring either weekly or bi-weekly reports. Next, their present scope should be expanded to include a report on minimization efforts and evidence of new crimes. Given the complexity of the minimization and retroactive-prospective amendment process, such reports would serve to facilitate compliance. Finally, the reviewing magistrate should be directed to suspend or terminate surveillance if the reports are deficient, evince serious procedural irregularities, or indicate that the legal basis for continued surveillance no longer exists. Such an amendment would promote close judicial supervision and ultimately serve to decrease the risk of electronic surveillance extending beyond its legitimate scope.

4. Preserving the Sanctity of the Tapes

Prior to the passage of Title III, numerous fears were expressed that taperecordings were too vulnerable to tampering to be admitted into evidence. Nevertheless, because of technological barriers, susceptibility to detection, and the availability of far easier ways by which to "frame" a defendant, these fears were generally regarded as unrealistic.⁷² Even so, Congress sought to preserve evidentiary integrity by requiring

that, "immediately upon...expiration...of the order, or extensions thereof," all tapes must be brought to the issuing magistrate and "sealed under his directions."⁷³ Further, the statute provides that the presence of this seal, "or a satisfactory explanation for the absence thereof," is a prerequisite to admissibility.⁷⁴

With some exceptions, this provision has only been loosely applied in the courts.⁷⁵ The adverse consequences, however have been negligible, for though the judiciary may be faulted for ignoring a statutory directive, the sealing rule presently serves little purpose. In reality, there is nothing sacrosanct about a "seal." Oftentimes, it is merely a piece of tape that is placed around the container in which the taperecording is stored. The tape used to effect the so-called seal may range from simple "scotch" tape to stronger cloth, adhesive-backed tapes. Regardless of which type is used, the tape usually contains a written notation indicating the sealing date and the sealing officer's signature. Together, however, the tape and written notations do little to protect the taperecordings' integrity. A forger would have a far easier time removing the tape than he would effecting a successful forgery of the taperecording. Moreover, even if the so-called seal delivered some magical protection to the taperecording, present Title III procedures do not advance this end, as the seal need not be secured until the eavesdropping warrant or extensions thereof have expired. Thus, at least theoretically, ample opportunity exists to tamper with the taperecording before the sealing requirement is even triggered.

Fortunately, allegations of tampering have never become a serious Title III problem.⁷⁶ Indeed, this probably explains the judiciary's

reluctance to enforce the current sealing rules strictly. And as the seal is of limited prophylactic value, absent dramatic technological advances in forgery techniques, the normal sealing requirement could be eliminated altogether - especially since the prosecution must still establish the accuracy of each taperecording prior to admissibility. Nevertheless, if sealing is to remain a statutory requirement, the present procedure should be modified to narrow the pre-sealing time period in which opportunity presently exists for forgery to be attempted. My suggestion is that the completed taperecordings be delivered for sealing and storage to the reviewing magistrate within 72 hours of completion. While this would entail frequent trips to the courthouse and administrative burdens for judiciary officials, it would be a realistic way to ensure the integrity of each taperecording. The 72 hour figure is suggested because investigators need sufficient time in which to make duplicate recordings (a process requiring only a few minutes for each taperecording, but which often consumes much more time because of transportation, manpower, and administrative difficulties). Finally, failure to comply should not automatically result in exclusion. So long as the taperecording accurately depicts the events in question, suppression should be reserved for situations involving repeated unexcusable delays.

5. Emergency Searches

The authors of Title III recognized that, on occasion, exigent circumstances would warrant electronic surveillance before an eavesdropping warrant could be obtained. Accordingly, warrantless emergency searches were authorized for situations involving national security interests or

the "conspiratorial activities characteristic of organized crime."⁷⁷ Such searches are permissible, however, only if all statutory requirements could have been met had time constraints not intervened, and provided that, within 48 hours of interception, an application is filed seeking retroactive approval for the eavesdropping.⁷⁸

Nevertheless, while a statutory emergency search procedure is clearly necessary, the present provision is simultaneously ambiguous, unduly narrow, and unnecessarily broad.⁷⁹ It is ambiguous because the statute does not define the term organized crime. It is unduly narrow because the provision does not extend to life threatening circumstances not involving national security or organized crime. Moreover, there are often other exigencies involving the need for warrantless surveillance. For example, a vehicle containing a hidden microphone device may cross jurisdictional lines, thereby technically suspending or terminating authorization to eavesdrop.⁸⁰ Obviously, under such circumstances, monitoring should be allowed to continue. Finally, the law is unnecessarily broad because there is no reason not to require oral notice to a judge before initiation of surveillance. As presently constituted, if an emergency search is unsuccessful, the risk exists that neither the judiciary nor the intercepted parties would necessarily be advised since no retroactive warrant may be filed.⁸¹ Moreover, given the considerable time usually required to initiate eavesdropping, there is usually no reason why oral judicial approval could not be obtained in advance.⁸²

Since enactment, Title III's emergency procedures have rarely been employed.⁸³ Because this may reflect inadequacies in the present law, the statute should be amended to rectify prevailing deficiencies.

Both law enforcement and civil libertarian interests would benefit as a result.

6. Standards of Review and Suppression for

Title III Violations

Passage of Title III was based upon a system of statutory controls which, with proper judicial enforcement, were designed to preserve Fourth Amendment rights. As much of my summary today indicates, however, statutory protections have often not been effectively implemented by the courts. To some extent, specific amendments can rectify this situation for future litigants, but such measures, standing alone, may be insufficient; historically, a result-oriented judiciary has demonstrated an inclination to gloss over specific statutory language or legislative history when the need to do so was perceived, and this tendency can be expected to continue when a reformed Title III is subject to interpretation. While such a judicial response cannot be absolutely controlled, it may be strongly discouraged by an explicit Congressional directive that, given the importance of the principles at stake, Title III is to be strictly enforced in the courts.

I should caution, however, that a statement of this kind should not be misinterpreted to the other extreme. It does not mean, for example, that every statutory violation merits the suppression of evidence: quite clearly, harmless errors -- those which are neither intentional nor "affect... substantial rights"⁸⁴ -- should not warrant this extreme sanction. Rather, it means that claims of misconduct must be evaluated honestly and rigorously in light of the important policies Congress sought to advance in passing the statute.

Finally, because the proposals I have advanced today would further complicate an already complex statutory process, less reliance should be placed on suppression for procedural errors. Presently, there is something anomalous about a society which seemingly demands perfection from few other than its law enforcement officials. In reality, the adage "nobody's perfect" applies to judges, prosecutors, and police officers as well as to everyone else; mistakes are an inevitable aspect of human life. Thus, as a general principle, it makes no sense automatically to exclude evidence -- and possibly the fruits of an entire investigation -- merely because someone has erred. And, in the context of a complex Title III, especially once reformed, it makes even less sense to do so. Instead, the focus should be on objective reasonableness and subjective good faith. More specifically, error should not occasion suppression so long as properly trained law enforcement officials have made reasonable good faith efforts to comply with the law.⁸⁵

This standard, standing alone, is a sufficient and sensible deterrent to official misconduct. Moreover, it can (and should) be reinforced through aggressive enforcement of Title III's criminal and civil sanctions which have thus far largely been ignored.⁸⁶ Of course, adoption of this standard, at least insofar as eavesdropping errors violative of the Fourth Amendment are concerned, is contingent on Supreme Court modification of the exclusionary rule in its present form. This issue will hopefully be addressed by the Court shortly.⁸⁷ Regardless of its outcome, however, the standard I have articulated will retain vitality for purely statutory violations of nonconstitutional dimension. Hence, the opportunity exists to add significant statutory protections without curtailing effective law enforcement.

CONCLUSION

Title III has provided law enforcement with an effective and constitutional means to achieve organized crime control. Years of experience under the statute have brought to light areas in which its original purpose must be restored as well as numerous improvements that are in order. Nevertheless, in considering reform, Congress should not undo the delicate balance between effective law enforcement and Fourth Amendment rights that was attained under the original legislative design. Indeed, only continued such equilibrium is consistent with the Fourth Amendment's intention to afford protection solely against "unreasonable searches and seizures."⁸⁸

NOTES

1. Goldsmith, The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance, 74 J. Crim. L. Criminology 1, 155-157 (1983) [hereinafter cited as The Supreme Court and Title III].
2. Electronic Surveillance: Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance 3, 11 (1976) [hereinafter cited as NWC Report].
3. See generally id. at 18; The President's Comm'n on Law Enforcement and the Admin. of Justice, The Challenge of Crime in a Free Society, 203 (1967).
4. See 18 U.S.C. §§2510(11), 2818(10)(a), 2515 (1976); The Supreme Court and Title III, supra note 1, at 40, 56-63.
5. 18 U.S.C. §2510(11) (1976).
6. 394 U.S. 165 (1969).
7. The Supreme Court and Title III, supra note 1, at 63.
8. Id. at 56-59.
9. Id. at 59-62.
10. Rakas v. Illinois, 439 U.S. 128, 136 (1976).
11. The Supreme Court and Title III, supra note 1, at 61.
12. See 18 U.S.C. §§2511 & 2520 (1976).
13. See The Supreme Court and Title III, supra note 1, at 61.
14. Cf. Franks v. Delaware, 438 U.S. 154 (1978).
15. Id. at 156.
16. See Wong Sun v. United States, 371 U.S. 471, 488 (1963); see generally Pitler, "The Fruit of the Poisonous Tree" Revisited and Shepardized, 56 Calif. L. Review 579 (1968).
17. 408 U.S. 41 (1972).

18. Id. at 47-51.
19. See The Supreme Court and Title III, supra note 1, at 71-73.
20. Id. at 73-75.
21. See generally Goldstock & Coenen, Controlling the Contemporary Loanshark: The Law of Illicit Lending and the Problem of Witness Fear, 65 Corn. L. Rev. 127 (1980).
22. The Supreme Court and Title III, supra note 1, at 72-74.
23. See United States v. Calandra, 414 U.S. 338, 342-44 (1974). See generally M. Frankel & G. Naftalis, The Grand Jury -- An Institution on Trial (1977).
24. See Katz v. United States, 389 U.S. 347, 355-356 (1967); Berger v. New York, 388 U.S. 41, 57 (1967).
25. 18 U.S.C. §2518(1)(c)(1976).
26. S.Rep. No. 1097, 90th Cong., 2d Sess. 66, reprinted in 1968 U.S. Code Cong. and Ad. News 2112, 2190. See The Supreme Court and Title III, supra note 1, at 130-31.
27. The Supreme Court and Title III, supra note 1, at 127-29.
28. Id. at 133.
29. Id. at 131-32.
30. See, e.g., Donnelly, Comments and Caveats on the Wire Tapping Controversy, 63 Yale L.J. 789, 804-07 (1954); Semerjian, Proposals on Wiretapping in Light of Recent Senate Hearings, 45 B.U. L. Rev. 216, 227 (1965).
31. The Supreme Court and Title III, supra note 1, at 90-92.
32. Id.
33. 415 U.S. 143 (1974).

34. 429 U.S. 413 (1977).
35. *United States v. Donovan*, 429 U.S. at 427, n.15; *United States v. Kahn*, 415 U.S. at 155, n. 15.
36. *United States v. Kahn*, 415 U.S. at 155, n. 15 (quoting *United States v. Fiorella*, 468 F.2d 688, 691 (2d Cir. 1972), cert denied 417 U.S. 917 (1974)).
37. *Katz v. United States*, 389 U.S. 347, 351 (1967).
38. The Supreme Court and Title III, *supra*, note 1, at 91.
39. *Id.*
40. *United States v. Kahn*, 415 U.S. at 157, n. 18.
41. *Cf. Ybarra v. Illinois*, 444 U.S. 85 (1979).
42. See The Supreme Court and Title III, *supra* note 1, at 103.
43. 18 U.S.C. §2518(5) (1976).
44. See the Supreme Court and Title III, *supra* note 1, at 53-54.
45. *United States v. Kahn*, 415 U.S. at 154.
46. The Supreme Court and Title III, *supra* note 1, at 104.
47. 436 U.S. 128 (1978).
48. The Supreme Court and Title III, *supra* note 1, at 110.
49. *Scott v. United States*, 436 U.S. at 136-139.
50. 18 U.S.C. §2518(5)(1976) (emphasis added).
51. The Court suggested, however, that once a violation has been objectively established bad faith may be a factor in determining the scope of suppression. *Scott v. United States*, 436 U.S. at 136.
52. The Supreme court and Title III, *supra* note 1, at 109.
53. *Id.* at 124.
54. *Id.* at 124-25.

55. This aspect of my proposed accommodation would not be operative if Title III's suppression sanction were subject to a good faith exception. See text accompanying notes 86-87 infra.
56. The Supreme Court and Title III, supra note 1, at 141.
57. See Texas v. Brown, 460 U.S. ____, 103 S. Ct. 1535, 1540, (1983); Coolidge v. New Hampshire, 403 U.S. 443, 465-467 (1971) (plurality opinion).
58. 18 U.S.C. §2517(5) (1976).
59. The Supreme Court and Title III, supra note 1, at 143-44.
60. Id. at 146-150.
61. Texas v. Brown 460 U.S. ____, 103 S.Ct. 1535, 1540, 1543-44 (1983).
62. The Supreme Court and Title III, supra note 1, at 143.
63. But see Texas v. Brown, 460 U.S. ____, 103 S.Ct. 1535, 1543-44 (1983) (suggesting that inadvertence may not be a feature of plain view doctrine).
64. 2 W. Lafave, Search and Seizure: A Treatise on the Fourth Amendment §4.11, at 179-80 (1978).
65. The Supreme Court and Title III, supra note 1, at 149.
66. Texas v. Brown, 460 U.S. ____, 103 S. Ct. 1535, 1540, 1543-1544 (1983).
67. See Michigan v. Summers, 452 U.S. 692, 697-700 (1981); United States v. United States District Court, 407 U.S. 297, 322-23 (1972) (reduced probable cause standard may be compatible with fourth amendment) v. See generally Racigal, The Fourth Amendment in Flux: The Rise and Fall of Probable Cause, 1979 U. Ill. L.F. 763; Greenberg, Drug Carrier Profiles; Mendenhall and Reid:

- Analyzing Police Intrusion on Less than Probable Cause, 19 Am. Crim. L. Rev. 49 (1981).
68. See generally 3 W. Lafave, supra note 64, §11.4(a), at 621-628.
69. The Supreme Court and Title III, supra note 1, at 44.
70. 18 U.S.C. §2518(6) (1976).
71. See The Supreme Court and Title III, supra note 1, at 136-37.
72. Id. at 15, n.81.
73. 18 U.S.C. §2518(8)(a) (1976).
74. Id.
75. The Supreme Court and Title III, supra note 1, at 151.
76. Id. at 158, n.944.
77. 18 U.S.C. §2518(8)(1976).
78. Id.
79. The Supreme Court and Title III, supra note 1, at 48.
80. See 18 U.S.C. §2518(3) (1976).
81. Since §2518(8) provides that, absent a court order, such interception violates Title III, the filing of an application and issuance of inventory notice to parties named therein is implicitly mandatory. Nevertheless, absent pre-surveillance judicial notification, it is difficult to ensure compliance with these requirements.
82. See N.J. Stat. Ann. §2A:156A-13 (West 1971).
83. See Wiretap Amendments: Hearings Before the Subcomm. on Criminal Justice of the Senate Comm. on the Judiciary, 96th Cong., 2d Sess. (Statement of Assistant Attorney General Philip B. Heymann).
84. Cf. 28 U.S.C. §2111 (1976). See The Supreme Court and Title III, supra note 1, at 82-83.

85. See U.S. Department of Justice, The Attorney General's Task Force on Violent Crime, Final Report 55 (1981). An objective component to the proposed good faith exception is necessary to prevent the new standard from fostering an atmosphere in which ignorance is implicitly encouraged.
86. See generally MWC Report, supra note 2, at 20, 23-24, 159-170.
87. See United States v. Leon, ___ U.S. ___, 103 S.Ct. 3535 (1983) (granting certiorari); Massachusetts v. Sheppard, ___ U.S. ___, 103 S.Ct. 3534 (1983).
88. U.S. Const., Amend. IV (emphasis added).

**TESTIMONY OF WILLIS H. WARE, CORPORATE RESEARCH STAFF,
RAND CORP.; AND ANTHONY G. OETTINGER, CHAIRMAN,
CENTER FOR INFORMATION POLICY RESEARCH, HARVARD
UNIVERSITY**

Mr. KASTENMEIER. Our next panel consists of Dr. Willis H. Ware, a member of the corporate research staff of Rand Corp. Years ago, he was with Rutgers Computers and Secretary Elliott Richardson. He also served on the Privacy Commission.

The second member is Anthony G. Oettinger of Harvard University. Mr. Oettinger is the chairman of the Program on Information Resources Policy at the university and is a leading expert on both computer sciences and the implications of new technologies on the freedom of information. Professor Oettinger additionally serves as consultant to the President's Foreign Intelligence Advisory Board of the National Security Council and numerous defense agencies.

Gentlemen, we have your written statements. Without objection, they will be made a part of the record, and you may proceed as you see fit.

Perhaps, Dr. Ware, you might like to go first.

Mr. WARE. Thank you, Mr. Chairman.

My credentials for addressing this subject are spelled out in the written testimony. You mentioned them, so I won't go over that.

I wish to state that I am speaking as an individual this morning, not as a member of the Rand Corp. I think what would be most useful from your point of view is just a hop scotch over a series of points and to highlight for you some of the technological issues that provide the context in which you are trying to deal with a very difficult and awkward subject.

First let me say the testimony we have had so far is technically a conversation about the past. The limitations about the manpower required to sit on wiretaps is a thing of the past, because we are now at the phase in the technology where one simply puts a computer on the intercept and it will mind the store for as long or for however one wishes. So the manpower issue will no longer be one in a few years.

Second, the terms, wiretapping, bugs, pen registers, are passé anachronisms. They are no longer useful, except as simple labels for a much larger problem that we need to talk about.

I don't need to dwell on the technology that is in the world today. It abounds. We all know that the common carriers of the country, the telecommunication carriers, use a wide variety of technology, microwaves, digital links, coaxial cables, satellite links, fiber optics, you name it, and that the traffic mix can exist either in analog or digital form. It is not news that voice can be digitized. It is being done by the telephone company regularly and has been done operationally since the early 1960's so that isn't news either.

At some point, though, I will point out that we had better worry about the cable networks which are really out on the end of the common carriers and extensions of them. The cable networks already carry much of the traffic that is on a common carrier, TV notably, but there is no reason why ultimately they also will not carry the same mix of traffic that the common carriers do. I might point out that the mix of traffic on the common carriers includes

not only voice conversations but video signals, electronic mail, facsimile, and data traffic too among computers.

A third point I would make for you is whatever media the communications employ, wires, coaxials, whatever, every one of them is interceptable in principle. Some are easier to do than others. Any that convey electromagnetic energy between antennas, such as microwaves or satellite links, are easy to do from afar, invisibly and without any permission from anybody needed.

Wiretapping, of course, in the legitimate sense of the word, required one to nuzzle up close to a copper wire pair, and is correspondingly harder to do.

So all of the information in transit in the common carriers of the country must be assumed interceptable in principle, whether it is in analog or digital form or whatever media is carrying it.

The congressional problem, as I see it, is to sort through a potpourri of conflicting issues to decide of all of the kinds of information that are on the common carrier's—voice, data, facsimile, TV, electronic mail, you name it—which deserve protection and then to specify how that protection shall be levied.

Now, in the course of doing that, you must take account of legitimate interests of other parts of Government, notably the intelligence community, the defense community and law enforcement, because they do have legitimate interests. And in doing that, you also must be careful to draft the legislation in such a way and to pay careful definition to meaning of words lest you create something which will be end run or out run by technology in a few years.

Now, I would point out that there is an overlap between your interests and the interests of other committees of Congress. You are concerned about information in transit and its unauthorized interception, which is the way we should think about it, or as controlled interception, perhaps.

But common carriers of the country use mechanisms which involve antennas, and historically mechanisms which involve antennas are the purview of the Communications Act and administered by the FCC. We are moving into an era in which the telephone network will have a mobile component which obviously implies antennas between automobiles and fixed bases. We already can go down to the local Radio Shack and buy portable handsets which you can carry around and are linked by radio transmissions to a base set. The blur between the interests, such as your subcommittee has, and the broader interests of communication protection is rapidly becoming very very muddy.

There is an obvious interface between your interests and the interests related to the Communications Act and also the interests related to privacy affairs, and I would hope that in your deliberation that these interfaces and interactions can be accommodated.

I would say it this way to you, the aspect of the problem in which you are currently involved is simply one dimension of a much larger, much greater general problem.

Now, what can you do about it? Looking at it from my point of view, as a technologist, you have several options. One is you can patch up the present Wiretap Act and take care of the comments and the objections that have been raised to it, and try to plug

whatever loopholes somebody thinks exist or you can fall back and do the homework that, in my judgment, is warranted.

To understand the situation, to carefully understand the utilization of technology and modern communications systems, to carefully understand the opportunities for unauthorized interception, to carefully judge which controlled opportunities you choose to allow and under what circumstances all represent homework that must be done. Then draft a re-do of the law with careful attention to the words and definitions and innuendoes.

So to speak, I think we as a country have to harmonize the information protection aspects in the Wiretap Act, in the Communications Act and probably in others. My druthers choice would obviously be the latter one. My point of view is "let's get the job done right and get it done in its entirety" and not be faced with having to come back and discuss it again and again and again every 5 or so years.

On the other hand, such revisits may be an unavoidable scenario because technology is moving so fast that none of us may have enough omniscience or vision to be able to anticipate and head off things 5 or 10 years out.

A quite different comment that I want to introduce, because Mr. Kastenmeier asked me explicitly to speak to it, is the subject of encryption as a possible technical approach to protecting information. It is true that techniques exist for encrypting both analog and digital information, and I would just point out in passing that generally speaking encryption is that body of mechanisms that can be used to hide information.

Unfortunately, the encryption technology for protecting digital traffic is much stronger than that for protecting analog traffic, but nevertheless, it does exist for both. The central issue is that to introduce encryption into the telecommunication carriers of the country would require a massive infusion of new capital and a massive retrofit of the installed plant.

In my judgment, therefore, encryption is not a practical approach to the issue that you are facing but primarily on economic grounds.

On the other hand, encryption is available to individual users. It could be, obviously, employed on a selective basis so that any one user of the common carrier networks who has enough concern about what he is transmitting over them can, of course, take his own measures to protect against whatever threat he believes he faces.

At the present time, though, the cost of providing encryption on a private or personal basis is relatively expensive. It is roughly \$10,000 for a link between here and there; \$5,000 for each end. The cost puts it out of the reach of the ordinary citizen and, therefore, to the extent that unauthorized or controlled authorized interceptions of communications take place, there is an invasion of privacy that the individual cannot protect against primarily because of the cost to his own sources.

Corporations, of course, regularly employ their own encryption technology. Banks notably can afford to do so, and they do so. So the bottomline on encryption is, yes, the technology is there. It is unreasonable and uneconomic to put it into the common carriers

on a large scale. Individuals can use it selectively but economically it is in the large unavailable to the individual person.

And I think with those comments, I would defer to my colleague, Tony Oettinger, and then we will deal with your questions, as you wish.

[The statement of Willis H. Ware follows:]

Testimony of

Willis H. Ware

INFORMATION AND COMMUNICATIONS PROTECTION

Before the Subcommittee on Courts, Civil Liberties and
the Administration of Justice, Committee on the Judiciary,
United States House of Representatives

January 24, 1984

INTRODUCTION

My name is Willis H. Ware. I am a member of the Corporate Research Staff of The Rand Corporation, but the views I state today are solely my own; they in no way reflect a position of The Rand Corporation or of its research clients. Furthermore, my views do not come from a specific research project, but rather reflect more than a decade of my attention to a set of issues of which communications security is one. I am an electrical engineer by training, but have specialized in the field of computer technology for over thirty years.

My credentials for addressing the issue include the following. In 1967, I was the first to bring the broad issue of computer security to the attention of the technical field by organizing a special session on the subject at a Joint Computer Conference in the spring of that year. Subsequently, I chaired a Defense Science Board (Department of Defense) committee to look at the issue of computer security which had never been examined comprehensively anywhere in government. The report was a definitive treatment of the subject, and to this day remains an excellent primer. Computer security, of course, involves communications security.

Because of my work in computer security, I was asked in the early 1970s to join a special advisory group to the Secretary of HEW, and I subsequently became its chairman. Its report, *Records, Computers and the Rights of Citizens*, was the first comprehensive treatment of the matter at the federal level. It provided the intellectual foundation for the Federal Privacy Act of 1974, which among other things created the Privacy Protection Study Commission of which I was a member and vice chairman.

Finally, as a practitioner of computer technology for some three decades, I must for professional reasons stay conversant with modern communications technology, and be aware of the concomitant security and privacy threats. I have participated in a variety of relevant workshops, committees, and task groups. Among them have been several for the Office of Technology Assessment.

In addition to my participation in the activities noted above, I have also spoken and written widely on the subject. In particular, I presented a paper, *Policy Aspects of Privacy and Access*, to a National Science Foundation symposium.¹

STATEMENT

Congressman Kastenmeier, it is a pleasure to testify before your committee this morning on a subject of importance to the nation. To make sure that we are on common ground, let me observe first that there are two dominant electronic technologies for information handling, namely computer technology and communications technology. In today's usage the two blend in almost every application. One finds computers in modern-day communications systems; conversely, one finds communications in contemporary computer systems. I would note particularly that contemporary communications systems are, in the large, computer-managed and computer-controlled. For our purposes this morning we can think of communications technology as the collection of technical mechanisms for electronically transporting information from place to place;

¹Published by Crane-Russak as a special double issue of its journal *The Information Society*, Issue 3/4, Vol. 2, in press.

in contrast, computer technology is used primarily to manipulate information in very general ways. It is important to pay careful attention to the meaning of words in our discussion because the two technologies have caused new interpretations of familiar concepts and phrases.

We are talking here today about electronic means for transporting information from place to place. We must insert the word **electronic** because there are other mechanisms for information transport, for example the postal carriage of printed materials.

A wide scope of technology is used in modern communications networks. The carriers who operate them employ traditional twisted-pair copper-wire circuits, microwave links, coaxial cable circuits, perhaps wave guide links, fiber optics increasingly, and communication satellites. In the future, perhaps even laser beams might be exploited for such things as short-hop circuits (say) across a river or between buildings of an industrial complex. In each instance the fundamental point of the technology is to convey electromagnetic energy from place to place; it in turn will be the vehicle for transporting information. I might observe parenthetically that the choice of technology in any particular instance is essentially an engineering consideration and balancing of such factors as cost of the installed link, its information capacity, the volume of information to be moved, and the long-time economics of revenue and cost recovery.

Technical opportunity for intercepting the electromagnetic energy-- and therefore the information which it carries--is not the same for each technology. For example, microwave and satellite circuits are more exposed in the sense that the energy is in transit through the atmosphere or space, and can therefore be intercepted from afar. Conversely, one has to get close to twisted-pair copper-wire circuits in order to capture its energy.

For the purposes of providing legal protection though, one must consider that any communications mechanism is interceptable in principle. I use the term "interceptable" as a generalization of wiretap.

Thus, there will flow a wide variety of information on circuits composed of a mix of such technology, all networked together by and among carriers. In the past the communications traffic, especially in the classical telephone networks, has been limited predominantly to voice conversations, but in today's world there is an ever increasing volume of data flow; so to speak, computer conversations. There will also be facsimile transmission of images from place to place; there will be video signals such as television, either for commercial distribution or for private use such as in teleconferencing; and on many circuits, particularly those having large transmission capacity, there will be a mix of such information types.

Frequently, information in transit will be represented, so to speak, in its natural form. Voice signals will be represented in transit as electrical ones that wiggle, and the wiggles will be a mirror image of the motion of the air molecules that transmit sound from lips to ear. Similarly, video pictures will probably also be represented in the so-called analog form. Information from computers, however, naturally comes in digital form and it will be transmitted that way, although if one could "hear" such data transmissions, it can sound like a sequence of tones.

On the other hand, much information will be changed from whatever its natural form happens to be into digital form. Voice, for example, may be transformed into a stream of digits which outwardly could be mistaken for a data stream from a computer; it has been digitized. Voice which has been transmitted digitally is then reconstructed to its analog form prior to delivery at the listener's ear. Theory clearly establishes that the reconstructed voice signal contains all of the information in the original spoken word. Commonly a facsimile system transforms the original image by some scanning process into a digital stream and reconstructs it at the receiving end by an appropriate mechanism.

Such are the common carriers of the nation, but out on the ends of their networks are the locally franchised cable networks. They carry many kinds of information now, and in the future can be expected to carry the same broad scope of information as will the common carrier networks--voice, data, television, facsimile, etc.

The Congressional problem is to decide how wide a blanket of protection to throw and what kinds of information warrant protection. Certainly, voice will be included as it already is, but it must be clear that the protection must exist whether the voice is represented within the communications network in analog or digital form. There are increasing volumes of data flow among computer systems of the industrial base, among computer systems of the research establishment, among the computer systems of government, among the computer systems of defense, and on and on. Such transmissions can obviously be of interest to eavesdroppers because they can reveal much about individuals, about corporations, about government, and about sensitive defense matters.

Congress could patch the 1968 Wiretap Act to bring data transmissions under its purview, but I would ask: Why do it piecemeal? It will only bring us back to this table in five or so years to address concerns about other kinds of information transiting the nation's common carrier system.

Even the phrase wiretap is inadequate and outmoded. It connotes the wrong thing because much of today's communications traffic is not carried on wires so one needs to consider some broader phrase such as communications tap or communications interception.

Suppose one does adopt a very broad point of view in order to avoid the risk that new law will be outrun by technology, and suppose one agrees that we really want to afford some measure of legal protection against the unauthorized interception of electromagnetic energy. Then, how does one distinguish between such energy flowing between (for example) microwave antennas owned by the telephone company and electromagnetic energy propagating between two antennas that sustain (say) international communications between the United States and some other continent or between any other two antennas? From a broad technical purview each is a carrier of information which can be intercepted. Distinguishing among them could only be done in some artificial way--which might, however, be desirable or essential from the viewpoint of law.

The point I want to leave with you is that information protection as now addressed in the Communications Act of 1934 and information protection that you will address in any revision of the 1968 Wiretap Act are but two aspects of the same general problem. One would suppose, therefore, that there is an important interface between the two items of legislation, and that some coordination must take place as the respective laws are revised. We must harmonize the concept of protecting information against interception across all pertinent law.

One clear option is to redo the 1968 Act in such a way that it is the legal basis for protecting against unauthorized interception wherever it occurs. A revised 1968 Act could, for example, accommodate any protective mechanisms that a revised 1934 Act might require. Clearly, another option is a minimum patch of the 1968 Act just to catch new technological developments, such as digitized voice, and to catch new kinds of information at risk, such as data flow or facsimile. If Congress chooses the latter course, however, I would urge that we be sure to review the matter again in five years or so lest technology again outruns or endruns law.

Clearly, my choice would be to do the whole job now, once and for all, and to get it off our minds. I do not see any risk attached to providing broad legal protection for any kind of information that is in transit on a communications channel implemented in any technology, and where the information can be represented in either analog or digital form.

I would note parenthetically that the analogous problem also plagues the copyright issue. For example, a movie first comes to the marketplace on film stock. Later the same movie will be transferred from film onto video cassettes or will be electronically transmitted to the viewer along cable television networks or over communication satellite networks instead of visually as in a theater. To whatever extent we wish to provide protection for the information contained on the original film base, such protection ought to be independent of whether it appears on film, on video cassettes, in transit along a CATV network, or over a satellite link. The protection is for the information, not for its fixation or its manner of representation.

Finally, I want to speak briefly to the subject of encryption which in effect hides information. Technically, protecting information by encrypting it is easier to do in the digital world than in the analog world. It is regularly done, of course, in defense communications for digital traffic, but analog information, such as voice conversations, will have first been converted to digital form. There are some things that can be done directly to analog information to protect it, but in general such mechanisms are not as strong as those that can be afforded to digital traffic.

The problem of protecting information in common-carrier communications networks by encrypting it is partly technical, but it is dominantly economic. To protect the common-carrier networks of the country by encryption techniques would require a massive retrofit of the installed plant, and it would require an enormous infusion of capital. Such protective encryption mechanisms, of course, could be done selectively, but then who is to say where an "intercept tap" threat will emerge? Moreover, even if done selectively, it is not likely that it would provide end-to-end protection--from the handset of the speaker to the handset of the listener--so the net effect of encryption would be simply to force the potential tapper to get closer to the handset for his activities. Eavesdroppers who could not get close enough to an unprotected end-link will, of course, be ruled out of the game.

A user can himself provide encryption capabilities if he wishes, but in the present state of art the cost of doing so is roughly \$5,000 at each end of the link. Thus the economic burden is out of reach for ordinary individuals.

For encryption the bottom line becomes:

- It is technically feasible--techniques do exist.
- It is extremely costly to do end-to-end.
- It would impact the common carriers enormously if mandated.
- It is out of reach for the ordinary individual.

It has been a pleasure to interact with you this morning. I hope that my views and my way of looking at the problem will be of value as you move forward on an issue which I consider to be of high import.

Mr. KASTENMEIER. Thank you, Dr. Ware.

I would just observe that obviously some of your questions and issues are more fundamental to this general hearing than the technical overview of whether title III is working or not. It is true that we are interested in but one dimension, or perhaps two, but that there are other dimensions. I suspect that we need to understand the other dimensions in order to correctly proceed with whatever responsibility this committee has.

We also, as you perhaps know, have the responsibility not only for the view of this in terms of wiretapping, overseeing privacy, but also for the purposes of copyright law. Although this particular hearing is not devoted to proprietary rights and copyright interests, we deal with new technology in some of the aspects you talk about even as far as whether encryption of one form or another is used by copyright interests as far as transmission of video material and other information.

And so we have at least that other dimension to ultimately accommodate or insure that it is not neglected in terms of a view of what is the state of affairs today, technology and indeed, if possible, a view of the future in this connection.

Mr. WARE. Yes, sir, I noted briefly in my written submission the analogy between the copyright issue and also the issues that you face here today.

Mr. KASTENMEIER. Dr. Oettinger.

Mr. OETTINGER. Mr. Chairman, thank you.

You mentioned in your earlier remarks concern for coherence. I think I can offer some notions of conceptual coherence that will help sort through the technological change. I tend to agree with Willis Ware that the application of whatever conceptual coherence there might be in this area is likely to have to proceed in a slow and painful area-by-area way, and I will get to that in a moment.

Let me summarize and highlight some of my salient points.

One, it seems to me that when you deal with privacy protection you need to go back to the fundamentals. One fundamental is that if you practice information birth control, then there is no need to protect information. In other words, if you shut up, there is nothing to be overheard and, if no records are kept, then there are no records to protect. I think many people forget that and many abuses occur when people shoot their mouths off when they shouldn't, and when agencies keep records when they shouldn't. I think lots of problems can be eliminated by backing up to those fundamentals.

If you must talk and must keep records, a second layer of questions surfaces: what is worth protecting? Not everything is worth protecting. Joan Rivers gives a good example many nights on the Johnny Carson Show. She clearly has no desire to keep her remarks to herself, so that the question of information birth control does not arise. As for "is it worth protecting?" when she asks, "Can we talk?" with her sort of quasi-furtiveness, and the answer is clearly, "Of course, we can," and then she shares pseudo-secrets with the nationwide audience, so the performance is a nice caricature, where there is neither desire for privacy nor for protecting what has been said.

Third, if information is worth protecting, there is a further question "against whom?", which is a very critical one, because different means may apply. The front end of this session seemed to deal with abuses by the U.S. executive branch, as if it were the only or the major enemy. I am not saying that there are no abuses by the executive branches of either the Federal Government or the State governments, but the notion that there are foreign powers who are of concern, that we ourselves in our private dealings are of concern, strikes me as of equal importance with abuses by the Federal executive branch. Hence, the "Pogoism" in my formal remarks to the effect that "we have met the enemy, and he is us" It seems to me that this is why the platitudes about external vigilance being the price of liberty remains of everlasting value; and as you pointed out in your introductory remarks, this branch of the U.S. Government has not been free of abuses in the past, as I too noted in my formal testimony.

Once we have decided first to avoid information birth control, second that some information is worth protecting, and third we know against whom it is worth protecting, then there still remains a question of will.

Only last comes technical possibility, since measures and countermeasures tend to keep pace with one another. Where there are new technical possibilities for intrusion, there are usually also possibility for protection, and vice-versa. I would agree with my colleague, Dr. Ware, that the questions are really price also the will to protect what is worth protecting. In my formal testimony, I give illustrations of allegations in the press, about the absence of will in conversations between the Secretary of State and the President of the United States. I also mention evidence rounded up in one of our studies that although a private data security industry has sprung up over the last decade or so, these companies are by and large overwhelmed by demand either from the private or the public sector.

Data security takes the back seat to life insurance or fire protection or most anything else, and my sense is that the Congress can perform a very important role by alerting the broader public to the need for some concern about information security and the need to decide about the layers of decisions about whether to say anything at all, and if so, it is worth protecting and so on. The idea of self-protection is a critical one, but people are not likely to do it, unless the circumstances are right.

Let me give one concrete example.

Mr. Ware alluded to the fact that major corporations can and do use encryption to protect themselves. That is usually practical within a limited range of points. Many of the problems arise, whether it is in the military or in corporate life, when the folks you need to get in touch with are not where the cryptographic equipment is. The tendency is to go in the clear, whether it is a bank money transfer, or a military operation. Whether through crypto-equipment or otherwise, there is the question of the massive investment that might be required to afford a broader—indeed universal—range of protection.

This is well-deserving of inquiry, because under the new competitive conditions the FCC and the courts have created within the

telecommunications industry and under the competitive conditions obtaining in the data processing industry, nobody is going to provide protection unless there is either a massive market demand that has to be satisfied and for which manufacturers and service providers can get a reward or some kind of mandate like safety standards in building codes or OSHA or fire protection or what have you, that require everyone to meet some minimal standards so no one in the marketplace will be handicapped by providing a high-priced product that no one will buy.

And so, the question of how to create market incentives that will create a demand, if you deem that it is worth doing, and then the means to meet that demand, I think, is something that deserves of attention at least equal to the attention given to revision of statutes on wiretapping.

On this matter of coherence in the presence of changing technology, let me suggest a notion that we found very useful with changing technology as a way of keeping an eye on the essentials. I won't elaborate on it here, since we are short of time, but I am happy to go into more detail whenever you wish. The point is to distinguish between the *substance* of information, *processes* whereby information is gathered, stored, manipulated and so on, and the *formats* in which that information appears to you, such as ink on paper or the little dots on the television screen or the electrical signals in a wire or signals going out over the air.

It is in formats that much of the technological change is taking place. Ink on paper may be replaced by TV screens. The processes are also changing: massive printing presses are yielding to various electrical devices, and instead of things being held in file cabinets and processed by hand, they are held in computers. But the substance of information, say, the information that it is raining today, might be put in any of these formats, ink on paper or TV, handled by different processes, the substance is what the name of the game is, that is what is worth protecting.

Only means change when the means for processing information and formatting it change. Substance and ends don't necessarily change. The problem with the laws—and I share with Dr. Ware the impression that some of the legal folks are burying us under a pile of dead leaves and fail to see the forest—is that while processes and formats are changing very rapidly, the laws are written in terms of obsolete formats and processes. They talk, for example, of wires and wiretaps, instead of talking about substance, the purposes that the substance serves, in what area, for what reason, commercial, national security and so on. It seems to me that by detaching the idea of substance, which remains fundamental, and the purpose of the substance, which is an area-by-area concern, from these rapidly metamorphosing processes and formats, it seems to me that by keeping those apart, may be a way to get some conceptual coherence while, at the same time, not burying every area under some often irrational statute.

Let me conclude by giving a concrete example of that going back to my formal testimony. Recordkeeping is sometimes a necessary aspect of a particular process. The reason why an issue arose 100 years ago between the Congress and Western Union was that the telegraph companies had to keep records of their transmissions be-

cause, otherwise, nobody would ever trust them to deliver the stuff correctly.

It was essentially a necessary part of the operation of that kind of a business.

Now, in old-fashioned telephone technology, there is no need for that. The stuff is always on the fly. With the more modern digital communications, we are coming back to a situation where, for operational reasons, there may be a need to store information again, which is why the whole notion of blanket prohibition against recordings, the treating of recording as interception, is absurd as a blanket idea.

There are times when it is operationally necessary, and there is no way of making sense of whether it is or is not, except area-by-area, and this delicate balance, conceptual coherence and the need to do area-by-area studies, it will keep you busy for a long time, Mr. Chairman.

Thank you.

[The statement of Mr. Oettinger follows:]

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Civil Liberties and the Administration of Justice

Hearings

1984: Civil Liberties and the National Security State

January 24, 1984

Testimony

of

Anthony G. Oettinger

Mr. Chairman, my name is Anthony G. Oettinger. I am a professor at Harvard University, where I chair the Program on Information Resources Policy. I am also a consultant to the President's Foreign Intelligence Advisory Board. The views I express here this morning are entirely my own, not necessarily those of any private or public organization with which I am associated; nor are they necessarily the views of any private or public organization that supports the research of the Program on Information Resources Policy (Biography and Affiliate List appended).

It was not George Orwell who said that "eternal vigilance is the price of liberty". Nor was this first said in 1948. Thomas Jefferson said it 200 years ago. So did one John Philpot Curran in the same era: "The condition upon which God hath given liberty to man is eternal vigilance; which condition if he break, servitude is at once the consequence of his

crime and the punishment of his guilt." Over 2,000 years ago Demosthenes put it: "There is one safeguard known generally to the wise, which is an advantage and security to all, but especially to democracies as against despots. What is it? Distrust." George Orwell is only the latest in a long and illustrious line.

You asked, Mr. Chairman, for my "assessment of the emerging technologies in the communications area and the potential hazards that they pose for the privacy of individuals". Big Brother can be anybody wielding many a tool fashioned from many a technology. These days we tend to see the Executive Branch wielding computers as Big Brother's most likely incarnation. In 1876, however, amid a struggle over the contested Hayes-Tilden election, it happened to be both chambers of Congress that plowed through telegraph company files searching for political weapons with which to capture the disputed electoral votes of Louisiana and Oregon.

When, on orders from Western Union president William Orton, the manager of Western Union's New Orleans office refused to reveal the contents of any dispatch, this House cited him for contempt. Shortly before, Western Union's directors had decided to arrange for "such speedy destruction of all written messages as the necessary keeping of accounts" would permit. The other telegraph companies and some newspapers applauded this seemingly principled stand for privacy. Western Union's customers were aghast. They argued that destroying the files would also make it impossible to hold Western Union's feet to the fire for errors in transmission, an intolerably frequent happening at the time. The files were not destroyed. By January 20, 1877 the New Orleans office manager was held prisoner in the Capitol, the ailing Western Union president was under arrest by a deputy congressional Sergeant-at-Arms and Western Union gave in to Congressional

subpoenas.

Technology had something to do with all of this. The telegraph system, unlike the telephone today, required fallible intermediaries, professional telegraphers, to tap out messages. Besides, the wires themselves were none too reliable. Recordkeeping was therefore thought to be essential for quality control. In the old-fashioned telephone technology which is still the run of the mill today, the only opportunity to catch messages is on the fly. A Charles Wick, a Richard Nixon, or a KGB agent has to run his own tape recorders, since phone messages do not have to be archived for day-to-day operating reasons, although operator supervisors do cut in from time to time to check on the performance of their charges. That intervention, sanctioned by law, has diminished in importance as more and more phone calls are being handled entirely automatically.

New digital communications (computer-and-communications) technologies have bloomed since World War II. These new technologies have destabilized the balances struck under an older order, just as their predecessors, like the steam-driven printing press or, for that matter, written instead of oral records, did in earlier times. In up and coming digital communications systems, for instance, there are many more nooks and crannies where a message can be netted, on the fly or on the branch, than in either the old fashioned communications systems or the isolated computer systems, which are becoming fewer and fewer.

At any moment in history it is a mix of politics, industrial organization and technology, among other factors, that determines how the privacy of individuals weighs in the balance with other values prized by both individuals and the society these individuals make up.

With newer technologies the interplays among technical, social and

political measures and countermeasures remain as complicated as ever and, above all, they remain reciprocal. Chicken Little, squawking predictions of a predestined doomsday, oversimplifies dangerously. So does puppy-like Pangloss peddling progress as best in the best of all possible worlds. By holding up visions of technology itself as satan or saint, both Chicken Little and Pangloss distract us from being vigilant over ourselves as the ultimate arbiters, fully responsible and in charge.

Doonesbury's cartoon ancestor Pogo, paraphrasing Perry's "We have met the enemy, and they are ours", joins Orwell, Jefferson, Curran and Demosthenes in correctly pointing at us, instead of suggesting that we bow to technological demons: "We have met the enemy, and they are us". Mr. Chairman, I will make plain what that means as I discuss, in response to your request, "the feasibility of protecting the privacy of individuals through the use of cryptography or other means of protecting personal privacy".

Feasibility is not the main problem. The very communications technologies that pour old risks into new bottles are also giving us more and more effective cryptographic means. There are many other means as well. And, ultimately, if you keep your mouth shut and nobody keeps tabs on you, then nothing needs encrypting. The least of our problems is how to protect what we agree needs protecting and what we agree we want to pay to protect. Our problem in the first instance is figuring out what needs to be said and what needs keeping tabs on. Second, our problem is figuring out what is worth protecting that has been said or that has been kept tabs on. Third, we need to muster the will to pay to protect what we think is worth protecting. Fourth, last and nowadays least, is the question of how to protect.

We give so much away that could be protected if technical feasibility were the main factor. Back in 1975, the Mayaguez incident needlessly cost the lives of a number of U.S. Marines when White House orders went through several secure satellite links only to be relayed to local force commanders in the clear. The enemy knew everything at about the same time as the U.S. commander on the site.

Only last year, October 22, 1983 to be exact, United Press International reported the following about the gunman who took Reagan aides hostage at the Augusta, GA, golf course:

"Monitored radio transmissions indicated the man hung up the first time Reagan called him. A minute or so later another call was placed and a voice apparently Reagan's came on the line.

'This is the president. This is Ronald Reagan. I understand you want to talk to me,' it said.

There was no response from the other end.

'Won't you talk to me? This is the president. If you are hearing me, won't you tell me and we can have that talk you want?'

The man, not yet identified, hung up a second time.

A short time later, the transmissions indicated the man told security agents he would not speak with Reagan by telephone and demanded to talk to the president in person."

This story is silent as to whether the monitoring was direct by the press, released to it, or fabricated. If fabricated, protection is not at issue. If released, protection was not wanted. If direct by the press, feasible protection either was not thought of or not thought important under the circumstances.

Technical feasibility does not seem to be at the heart of the matter, if one can believe the following account, in The Washington Post of April 17, 1982, of Jack Anderson's published intercept of a conversation between President Reagan and then Secretary of State Alexander Haig:

"Government communications specialists said last night it is not unusual for the president or a Cabinet secretary to forego the

use of a secure telephone and talk over open lines, especially if the connection is between two remote spots.

The sources said the intercepted conversation was initiated by Haig, who had a secure telephone on his Air Force plane but elected not to use it.

'They do it all the time,' one government security official said, despairing of the reluctance of officials to use the large, cumbersome, box-like apparatus that scrambles conversations at one end and decodes them at the other.

Another administration source said both men were advised before the conversation that they were not using a secure line, and both agreed that it was not necessary.

The specialist speculated that Haig and Reagan talked over a high-frequency connection that would be easy for ham operators to intercept."

In 1975 the late Nelson Rockefeller, in the name of a Commission that included a political commentator and former President of the Screen Actors' Guild named Ronald Reagan, wrote that "Americans have a right to be uneasy if not seriously disturbed at the real possibility that their personal and business activities which they discuss freely over the telephone could be recorded and analyzed by agents of foreign powers". And, according to David Burnham's December 19, 1983 New York Times article that you sent me with your invitation, Mr. Chairman, "The Carter Administration took limited technical steps to prevent the Russians from obtaining sensitive Government data and ordered the National Security Agency to help private corporations improve their security. But it never took any formal legal action against the Russians or formally asked Congress to amend the law".

Although something of a private data security industry has sprung up over the last decade, a study that the Harvard Program on Information Resources Policy published in 1982 indicated that these companies were underwhelmed by demand from both the private sector and the government. I have no reason to think otherwise today. Demand to protect either the conversations of the President of the United States or Aunt Minnie's confidences seems to lag behind demand for both smoke detectors and life insurance. And, surely, when Joan Rivers asks "Can we talk?", she is not pleading for privacy. Mr. Chairman, we have met the enemy, and they are us.

References

- Allen, Ira A. "Gunman - Augusta, Georgia," United Press International, Oct. 23, 1983. BC cycle.
- Burnham, David. "Loophole in Law Raises Concern About Privacy in Computer Age," The New York Times, Dec. 19, 1983, Section A, p. 1.
- Ferguson, Tom. Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography. Cambridge: Program on Information Resources Policy, Harvard Univ., 1982.
- Lipscomb, Greg. Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points. Cambridge: Program on Information Resources Policy, Harvard Univ., 1979.
- Seipp, David J. The Right to Privacy in American History. Cambridge: Program on Information Resources Policy, Harvard Univ., 1978.
- Seminar on Command, Control, Communications and Intelligence. Guest Presentations - Spring 1980. Cambridge: Program on Information Resources Policy, Harvard Univ., 1980
- Taylor, Paul and George C. Wilson. "Al, Hello, Al . . . !; Haig-Reagan Phone Call, on Open Line, Intercepted," The Washington Post, April 17, 1982, First Section; A1.
- U. S. Commission on C.I.A. Practices. Report to the President by the commission on CIA Activities Within the United State. . Washington: Government Printing Office, 1975.

Program on Information Resources Policy

Anthony G. Oettinger
 John C. LeGates
 John F. McLaughlin
 Benjamin M. Compagnone
 Oswald H. Ganley

ANTHONY G. OETTINGER

Chairman, Program on Information Resources Policy
 Chairman, Center for Information Policy Research

Anthony G. Oettinger is Gordon McKay Professor of Applied Mathematics, Professor of Information Resources Policy, and a member of the Faculty of Government at Harvard University. He is a consultant to the President's Foreign Intelligence Advisory Board and a member of the Scientific Advisory Group of the Defense Communications Agency.

He was chairman of the CATV Commission of the Commonwealth of Massachusetts (1975-79) and a member of that commission from its creation in 1972. He has served as a consultant to the National Security Council (1975-81) and to the Office of Science and Technology (1961-73). He has also been a member of the Command, Control, Communications and Intelligence Panel of the Naval Research Advisory Committee (1978-82), a member of the Research Advisory Board of The Committee for Economic Development (1975-79), and a consultant to Arthur D. Little, Inc. (1956-80).

He is a member of the Council on Foreign Relations and a Fellow of the American Academy of Arts and Sciences, the American Association for the Advancement of Science, and the Institute of Electrical and Electronic Engineers. From 1966 to 1968 he was president of the Association for Computing Machinery. He was chairman of the Computer Science and Engineering Board of the National Academy of Sciences from 1967 to 1973.

Professor Oettinger wrote, with Paul Berman and William Read, High and Low Politics: Information Resources for the '80s, Ballinger Press, 1977. He is the author of Automatic Language Translation: Lexical and Technical Aspects, of Run Computer Run: The Mythology of Educational Innovation and of numerous papers on the uses of information technologies.

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University

Center for Information Policy Research

Contributors

Action for Children's Television
 American Broadcasting Companies, Inc.
 American District Telegraph Co.
 American Telephone & Telegraph Co.
 AT&T Information Systems
 Arthur D. Little, Inc.
 Auerbach Publishers Inc.
 Automated Marketing Systems
 Bell Telephone Company
 of Pennsylvania
 Booz-Allen Hamilton
 Canada Post
 CBS Inc.
 Channel Four Television Co. (Ltd.)
 (United Kingdom)
 Citibank N.A.
 Codex Corp.
 Communications Workers of America
 Computer & Communications Industry Assoc.
 COMSAT
 Continental Cablevision, Inc.
 Continental Telephone Corp.
 Coopers & Lybrand
 Copley Newspapers
 Cowles Media Co.
 Cox Enterprises Inc.
 Dialog Information Services, Inc.
 Digital Equipment Corp.
 Direction Generale
 des Telecommunications (France)
 Diversified Communications, Inc.
 Doubleday, Inc.
 Dow Jones & Co., Inc.
 Drexel Burnham Lambert Inc.
 Dun & Bradstreet
 EIC/Intelligence Inc.
 Federal Reserve Bank of Boston
 First National Bank of Chicago
 France Telecom (France)
 Frost & Sullivan, Inc.
 Gannett Co., Inc.
 Gartner Group, Inc.
 General Electric Co.
 General Telephone & Electronics
 Hallmark Cards, Inc.
 Hambrecht & Quist
 Harte-Hanks Communications, Inc.
 Hazel Associates
 Hitachi Research Institute (Japan)
 Honeywell, Inc.
 Hughes Communication Services, Inc.
 E.F. Hutton and Co., Inc.
 Illinois Bell
 IBM Corp.
 Information Gatekeepers, Inc.
 International Data Corp.
 International Resource Development, Inc.
 Invoco AB Gunnar Fergvall (Sweden)
 Irving Trust Co.
 Knowledge Industry Publications, Inc.
 Kokusai Denshin Denwa Co., Ltd. (Japan)
 Lee Enterprises, Inc.
 John and Mary R. Markle Foundation
 MCI Telecommunications, Inc.
 McKinsey & Co., Inc.
 Mead Data Central
 MITRE Corp.
 Motorola, Inc.
 National Association of Letter Carriers
 NCR Corp.
 National Telephone Cooperative Assoc.
 New Jersey Bell
 New York Times Co.
 NEC Corp. (Japan)
 Nippon Telegraph & Telephone Public
 Corp. (Japan)
 Northern Telecom Ltd. (Canada)
 Northrop Corp.
 NYNEX
 Ohio Bell
 The Overseas Telecommunications
 Commission (Australia)
 Pearson Longman Ltd. (United Kingdom)
 Pitney Bowes, Inc.
 Public Agenda Foundation
 RCA Corporation
 Reader's Digest Association, Inc.
 Research Institute of Telecommunications
 and Economics (Japan)
 St. Regis Paper Co.
 Salomon Brothe.*
 Satellite Business Systems
 Scaife Family Charitable Trusts
 Seiden & de Cuevas, Inc.
 Southern Pacific Communications Co.
 Southwestern Bell
 Telecommunications Research
 Action Center (TRAC)
 Time Inc.
 Times Mirror Co.
 Times Publishing Co.
 TRW Inc.
 United Parcel Service
 United States Government:
 Central Intelligence Agency
 Department of Commerce:
 National Oceanographic and
 Atmospheric Administration
 National Telecommunications and
 Information Administration
 Department of Defense:
 Office of the Under Secretary of
 Defense for Policy
 Department of Energy
 Federal Communications Commission
 Internal Revenue Service
 National Aeronautics and Space Admin.
 National Security Agency
 United States Information Agency
 United States Postal Rate Commission
 United States Postal Service
 U.S. - Japan Foundation
 U.S. West
 United Telecommunications, Inc.
 Warner Amex Cable Communications Inc.
 Warner Communications, Inc.
 The Washington Post Co.
 Western Union
 Wetters Samson Group (Holland)

Mr. KASTENMEIER. Thank you.

I am not sure how helpful that is in the sense that I think you have said that it would make it almost impossible to resolve these matters in some sort of statutory concept ultimately.

It is like a moving target, in terms of some sort of statutory fixing of what it is we are treating, and while it is useful to say, we need to consider the new language, and perhaps modify our statutory language accordingly, that language, too, presumably is changing so quickly that it would be difficult for us to keep any statutory forms up to date on these subjects.

Do you have any specific advice to us specifically, in terms of how we might respond to an impossible task?

Mr. OETTINGER. I meant to be very concretely helpful by suggesting that you focus on the substance of the information, the nature of the data that are gathered or stored and that have to be protected and focus less on the details of means, that is, focus less on formats and processes.

The problem is with words like "wiretap." Likewise in the copyright matters, which I have followed for 20 years, the specificity of language dealing with ephemeral technology rather than with the information itself, the intent of the property rights in the substance of information.

Mr. KASTENMEIER. Is the language of content or substance necessarily constant and unchanging?

Mr. OETTINGER. Less changing than the language of processes or formats. That is exactly my point.

Mr. WARE. There are positive attributes of what he has suggested. It is always easier to do a smaller thing than a bigger thing, so to speak carve the problem up into kinds of information and approved uses. It would fragment the issue into a series of smaller things which we could deal with intellectually better and build a case better.

The privacy area, the Fair Credit Reporting Act, on and on, are essentially this approach: Each body of information may be used for specified things, and it is supposed to be protected in these ways; but you run into the following problem:

The 1976 tax law stipulated that all tax information is confidential, and therefore, it is supposedly protected as such.

The IRS transmits large volumes of tax information all over the country, but it has no way to protect it while it is in transit, so there is a technical violation that is unavoidable.

The law says one thing, but technology won't economically permit it to happen. In principle, the IRS could buy a lot of encryption boxes, but they were not available in 1976; they could provide their own protection. Even if we slice the pie up and try to deal with this and that body of information, if any one of them finds itself on the common carriers of the country, you still have the problem of protecting it or deciding whether it needs to be protected; and if so, what are the circumstances under which it may be intercepted and used.

The problem centers around the ability of the telecommunication carriers to protect or not to protect what is in their hands.

There is one carrier, Satellite Business Systems, which does offer a specific tariffed service encrypted end to end—from me to you, it is protected.

The stories are to the effect that there are not very many takers of the service. People fail to see the threat; corporations fail to see it. They simply are unwilling to pay the differential cost for the protection.

Mr. KASTENMEIER. Let me ask you this on that issue of encryption, taking a private corporation may, if it desires to protect its transmissions by encryption or some other method, in the ultimate, it is not able, I take it from, if one understands the very substantial involvement of the National Security Agency, in terms of the funding and development of encryption, to ultimately protect itself from the Government, that is to say, because, am I not correct in assuming that they sit at the top of the apex in terms of encryption for which this country is technologically responsible?

Mr. WARE. Yes, but there is available a so-called Digital Encryption Standard, DES. It is a matter of public knowledge that the NSA played a part in certifying the encryption standard.

The National Bureau of Standards has a series of documents telling how to use encryption, and the best commercial products are built around that scheme.

If you take evidence available in the public record and add to it what you hear in the halls at computer conferences, the DES is a valid approach for providing encryption standards for the foreseeable future.

Mr. OETTINGER. That cat is long out of the bag.

The means for computer-and-communications security, shortening that to communications security, are in the public domain and no longer in the monopoly of the United States or any other Government, so I think that that has become a red herring.

Much more serious is the absence of will, of a market demand. Plus insistence on perfection. Let me go back to something more familiar, which is fire protection.

You can buy yourself a strong box that may resist a 5-year-old trying to appropriate a bit of money for candy, but won't resist an adult with a screwdriver and a pen knife. You can buy a more elaborate filing cabinet with a lock and key, and then there are safes that are rated to resist an hour or so against a professional burglar or a small fire and you pay more for ones that will drop 10 stories and be in an inferno for 10 hours and still protect what is inside them.

The protection of information should be looked at in exactly the same way. There are gradations of threats, gradations of protection and just because we can't have the ultimate of protection, that doesn't mean we ought not to protect ourselves against obvious intrusions. The question of whether, in the common good, some minimal—and little-by-little increasing—standards of protection should be mandated for services of common concern, namely, the aggregate of the common carriers of the United States, is something that would be very appropriate for the Congress of the United States to consider.

Mr. KASTENMEIER. Again, that analysis is correct insofar as corporate entities are concerned. It doesn't seem, however, to deal

with the passive U.S. citizen and his or her ability to protect such a person against intrusions, because they do not take such factors into consideration.

There is an expectation of privacy which is easily violated because they do not take precautions to protect themselves. They are not able to financially or otherwise.

Mr. WARE. The people who have computer conversations back and forth can take care of themselves. They can agree to do encryption, and they can take care of themselves. It is the private citizen that is at bay.

It is very, very expensive, if not bordering on technical impossibility, to provide protection end to end.

Mr. OETTINGER. If we do not take minimal steps in that direction, we will never get there.

We are entering a couple of decades of the evolution of the national telecommunications network into a digital form. In that process, incremental investments to afford that kind of protection to every citizen, I think, are feasible if there is a will. Otherwise it will not be done because being everyone's business it is nobody's business. With the dissolution of AT&T on January 1, and with the competition in that area over the last decade, it has become less and less of anybody's business.

Unless the Congress of the United States at some point says there is a mandate for the private sector to increase—gradually so the investments are affordable—the degree of protection available throughout the communications network by all competitors so nobody is disadvantaged, without that happening, your nightmares will continue to be nightmares.

Mr. WARE. We are moving gradually to an all-digital telecommunications scene in this country, and therefore, the technical feasibility of gradually building in protection as we go is there.

Mr. OETTINGER. What is needed is incentives.

Mr. WARE. However, whatever the telecommunication carriers do by way of building in that kind of protection, for a long, long time beyond when they get their job done, that wire between the telephone pole and your house will continue to be vulnerable.

Mr. KASTENMEIER. One of the problems confronting the Congress, it seems to me, is how we proceed, as, Dr. Ware, you suggested at the outset, because this is a fractionalized question of how we deal with the new technology in communications, whether it is for what purpose; one subsidy may have computer crime and another may have a difference aspect, and I am not suggesting the answer to this question is yes. I have to raise it anyway.

With that in mind, do you see any need for some special select commission to deal comprehensively with the problem, or indeed with its various aspects it may not be easy to deal with?

Mr. WARE. I had personal experience with one. I am convinced that for some problems a commission approach is a very good mechanism that the country can employ. It is very useful for problems which cut across jurisdictions of interest, very good for problems which crop up here, there, and everywhere, but are basically just different aspects of the same thing.

So yes, I am on record in more than one place of touting some sort of a congressional, not Presidential, commission to examine

issues. What do we ask it to do in terms of scope and breadth? That is a very subtle choice.

Mr. OETTINGER. Commissions come and go. My sense is that over the longer term, some kind of joint congressional committee that might oversee the strategic side of this, leaving the area-by-area application to particular committees and particular fields, might be a way to approach this. The commission idea is at best a stopgap, but perhaps a very necessary first step.

Combining overview and coherence with area-by-area specificity is the only way to go, because if we go just area by area, there will always be cracks and those cracks will be precisely where we are vulnerable. That is where the information will be stolen, between the cracks, and if we go just overview, we will keep on fiddling while Rome burns.

Mr. WARE. This is true, and in part is the explanation of why a contemporary company will always have a vice president for data processing and communication matters. Somebody is in charge of it.

One needs to put the information infrastructure in somebody's hands to be minded; and in the long run, we could well try to be innovative about doing so at the national level. Suggestions for doing so in fact might be one charge that you could lay on a commission, to come up with a sequence of options for putting somebody in charge.

Mr. OETTINGER. It is a blind spot in our whole Government.

The brawn and muscle people, whether it is within the military, in the Defense Department themselves, or their academic hangers-on and so forth, are very strong, and very minimal attention is paid to the brain side.

It is only within the last few years that minimal attention has been paid to that, and in the appropriations process, if it is a matter of hardware and munitions versus command and control, the information side will always get the short end of the stick. We understand energy and materials, but we don't pay enough attention to the information side of the things that make our organizations tick.

Mr. KASTENMEIER. I fear that is true, and in fact it is obvious that while this committee is concerned, among other things, in part with the possible intrusion by the Federal Government in terms of the people, on the other side are the concerns of national security interests.

The point of these conflicting, not reaching Big Brother in the 1984 state, assuming we have to participate fully in the utilization of the technology, is a very different question.

I thank both of you for your appearance today. I hope that some of your suggestions and your advice to us we will take advantage of, and I want to compliment you both.

Mr. WARE. We are both available for further discussion whenever Mr. Beier or others wish.

Mr. KASTENMEIER. One thing I would ask of perhaps both of you, and that is, what are the dimensions, as you see them? Spell them out. Only some of the dimensions will concern us directly, but we need to be aware of the other dimensions to the question. See if

you can conceptualize it more generally in letter form to us, and this would be very useful to us.

Mr. OETTINGER. Very good, Mr. Chairman.

Mr. KASTENMEIER. I would hope that Ms. Bok, our next witness, who has been very patient, would indulge the Chair in a 10-minute recess. Perhaps I can get some of our other colleagues to join us.

[Recess.]

Mr. KASTENMEIER. The committee will come to order.

Our last witness this morning is Sissela Bok, who is the author of three books, "The Dilemma of Euthanasia: Moral Choice In Public And Private Life," and "Secrets On The Ethics Of Concealment And Revelation." These works, particularly the latter two, raise important, serious, moral and philosophical questions.

Particularly of interest to us are the distinctions between the right to know through the Government disseminating information and the dissemination of personal information to the Government and to other strangers.

We have seen a tendency to limit access to Government information, and on the other hand there may be a growing tendency by Government to gather more personal information on individuals and to use it for purposes unrelated to the original justification. Each development produces conflicts.

We are very pleased and delighted to have you here. We apologize for the delay in reaching you as a witness this morning. We invite you to proceed as you wish.

TESTIMONY OF SISSELA BOK, AUTHOR OF "SECRETS" AND "LYING;" PROFESSOR, HARVARD UNIVERSITY

Ms. Bok. Well, Mr. Chairman, thank you very much for your indulgence in having me come later. My plane was being de-iced and there wasn't very much I could do at the Boston airport.

I have been asked to come here and talk about the problems that your committee faces and to give some of the views in my book "Secrets" that you mentioned earlier. That book does tie together the two concerns that your committee is concentrating on, the concern about Government keeping more and more secrets, and about Government and other individuals and other organizations probing into more and more information that private citizens would like to keep private.

I think that the work of your committee is exceptionally important, and I would like to say in response to one of the questions that you addressed to another witness that I do believe there would be a place for a commission, perhaps even two commissions, to address the two mirror images of this problem that you are confronting.

It may be that one commission might not be able to cope with both, and I would say that each of the commissions or the commission, if it is the same, should then have to look into every single different proposal that is being made, every single new measure of secrecy or of probing that has been instituted.

I think 1984 will be an exceptionally important year for the decision with respect to Government control over information in the

United States, both control over its own information and control over information that private citizens may dispose of.

I don't think that we are in any danger of coming close to the Oceania of 1984. We have our traditions of free speech and of a free press and we do have a number of restrictions on official secrecy; but the pressures for secrecy and more secrecy are strong and never more so than when national interests increase so far as they have in the last year.

The administration in confronting the Soviet Union, a government that does exercise pervasive secrecy and censorship, is now moving to reciprocate. It is as if it were trying to catch up in the secrecy race as strenuously as it pursues the arms race.

Technological change is coming so rapidly that both protecting and intruding into secrets take on new dimensions.

Every government that tries to keep more secrets from citizens also tends to pry into more information about citizens. I think that is almost a law of nature that one might like to establish. And in a democracy, of course, the burden of proof has to be on the government to justify every increase in secrecy that it attempts to secure, and the burden of proof also has to be on the government to justify every new intrusion into the affairs of private citizens.

Those who have testified before this committee earlier have spoken of the many different ways in which the government is pressing this secrecy race: through press censorship, as in the invasion of Grenada, through measures to limit the Freedom of Information Act, and through expanded powers to classify information as secret, as well as through limits on travel, research, publication, and commerce in the private sector.

Perhaps the most dramatic and far reaching of the new efforts to control information is to be found in the national security Presidential directive of March 11, 1983. These many measures must be looked at together in order that their full force be grasped. They risk imposing direct Government controls over what millions of Americans write and speak, not only in public service but in the private sector; and I believe that the indirect effects of such controls will be felt by all Americans, because the indirect effects will have to do with all kinds of legislation and all kinds of Government measures.

Why should the United States, of all countries, with its traditional distrust of official secrecy, be moving in this direction? In a way the reasons are in one sense easy to understand.

Faced with the extensive controls over information, travel, research, and trade exercised by the Soviet Union and other countries, leaders of the Western democracies experience a dangerous imbalance, made all the more troubling now that the arms race and rising international tensions have so greatly increased the danger of armed conflict.

In addition, the new technologies of intelligence—the methods of surveillance and photography, the satellites and the spy planes—have made all nations feel that their secrets are more vulnerable than ever.

While these motives are understandable, and I know your committee is taking them seriously, the drawbacks of tightening official secrecy should give pause. In the first place it has not been

shown how the new measures will increase security. Just how will censorship in Government and science, for instance, guard against the new technologies of surveillance? And even if such censorship could be enforced domestically, how would it avail against the flow of scientific and technological information, often of the highest order, between other countries? We are not the only country with this kind of advanced information.

As for leaking, does anybody really believe that lie detector tests will do much to arrest it? So long as high officials leak with impunity, others will follow suit; and at times leaks are of the highest importance to the public—as in the many revelations that exposed the Watergate abuses.

Indeed, official secrecy and leaking exist in a symbiotic relationship; for as Government secrecy expands, more public officials become privy to classified information and are faced with the choice of whether or not to leak, at times when they think an abuse or something problematic is going on; growing secrecy likewise causes reporters to press harder from the outside to uncover what is hidden. And then, in a vicious circle, the increased revelations give Government leaders further reasons to press for still more secrecy.

Advocates of the stepped-up secrecy may agree that it is unlikely to do much for security, but conclude that nevertheless it is worthwhile even if it has only a limited effect—perhaps a chilling effect on at least some would-be leakers, for example, or a timelag before the public learns about military ventures abroad.

In so doing, however, these advocates often ignore or play down the second drawback of increased secrecy: the risks it carries for the Nation, which I believe are very serious. A look at secretive societies around the world shows that insofar as governments manage to impose official control over what is written, over research, over travel and public service, they undermine the most fundamental freedoms.

The control, moreover, affects not only national security but, much more often, what would present a challenge to government leaders themselves: all that might prove embarrassing, all that stands in need of challenge, all that exposes failure and wrongdoing.

Now, political life in our country depends crucially on how the public perceives officeholders. They operate under the strongest pressures to avoid exposure of anything that would leave them open to criticism. It is folly to believe that the power to censor and control information would be restricted to legitimate national secrets. It never has and it never will.

To such warnings, proponents of tighter Government controls might well retort that they intend to steer clear of all abuses of secrecy and all risks to the Nation. But in the absence of explicit and adequate safeguards, this reply is entirely beside the point. No one, however well intentioned, can know in advance how future American Governments will use the secrecy and censorship provisions, once they are enacted. Nor can anyone guarantee that all those who exercise the new controls will be immune to the corrupting effects that secrecy—like all other exercises of power—can have.

The risks of secrecy are especially great when allied to unusual political or other power, and greatest of all when it is in the hands of government leaders. Because official secrecy allows governments to deceive and manipulate public opinion without any accountability whatsoever, it cuts at the very roots of democracy. It prevents citizens from perceiving and debating the issues, and often gives a false sense of their simplicity, suggesting that all is fine when it is not—as when our Nation was misled by an elaborate system of secret double-entry bookkeeping into ignoring the U.S. bombardment of Cambodia during the Vietnam war.

The effect of the new measures on public debate would be devastating. Look back, for example, at the past month's op. ed. articles in a number of national newspapers written by former public officials, including such strong critics of present policies as Averell Harriman and Ambassador Robert White. How many would bother to write if they had to depend on advance clearance? And how many would receive it speedily enough for their comments to have timely impact?

Official secrecy and the silence and the manipulation it allows undercut what Simone Weil called "that interval of hesitation, wherein lies all our consideration for our brothers in humanity." It is this interval of hesitation, of reflection, of timely debate, that permits citizens to think about what they owe to one another and to citizens of other nations.

Along with such risks to our democratic process, the new measures carry risks to the individuals on whom they are imposed. Scientists and others have already testified about their concern that censorship will dissuade some of the ablest among them from entering fields or undertaking research threatened by censorship.

And here I would like to add that only 2 days ago in the Boston Globe it was reported that there had been a survey of the scientists who worked for the Manhattan Project in World War II. Every single one of those interviewed said that they would not have joined that project if they had been asked to sign a prepublication review agreement—every single one. So that if we are interested in national security, this is a point to take into account.

I predict that the same will happen with respect to persons in Government service, already burdened by harassment and lowered income by comparison to past years. I base my prediction on conversations with both actual and prospective Government employees. Their distaste for the new directive is striking, as is their sense of its adverse implications for their own lives, and you can understand why.

Put yourselves in the place of someone wondering whether or not to seek Government employment—perhaps for a few years only to begin with. Would you not think twice about accepting a position that would subject you to prepublication review for the rest of your life?

Our country can ill afford losing the services of those with enough independence and foresight to resist the thought of such lifetime censorship: those who think about their entire life and the restriction that censorship would place upon it, and about the many different kinds of Governments that this country may have in the future.

We are not always going to have the Government that is proposing these measures and other Governments may have unforeseeable ideas about the secrecy provision.

If the new measures dissuade but a portion of able men and women from undertaking scientific research or going into top level Government service, national security will be injured, not helped.

Given these threats to our democratic process, to individual liberties, and to national security from the new secrecy provisions, it is imperative that each one receive the most careful examination. And this must happen before, not after, they have taken hold; for alas, it is much easier to institute such practices than to end them.

We have to take seriously the claim that more secrecy is needed, but by itself the claim cannot suffice. We must be shown instances of the dangerous revelations thought to have harmed national security so severely as to subject the Nation to the unprecedented new measures.

So far as I know, advocates of the new regulations have produced no compelling set of such instances. Some have even argued that it would damage the Nation's security interest to mention them at all. This will not do. Neither Congress nor the American public can be asked to accept the tightened secrecy on faith, without detailed demonstration of the evils it is supposed to remedy.

Only when the evidence is produced will it be possible to examine it critically. Until then, I think we have to ward off every single measure that asks us to take things on faith.

It will then be possible to consider just what dangers to national security are in question, and to ask how the stepped-up official control is meant to remedy them, whether it is likely to do so, what risks accompany each new measure, and what alternatives might better serve genuine national security.

In so doing, it will be important to consider yet a third reason to question the new secrecy measures, one that is international in scope. It concerns the role that secrecy plays in fueling the arms race.

Every nation obviously needs a degree of secrecy for self-defense; yet most States use far more of it than is needed for purposes of defense. Throughout the world, secrecy is a weapon in the hands of aggressors and an aid in every scheme of internal repression; and secrecy between nations has come to play a dominant role in increasing the distrust and suspicion that fan regional wars and propel the arms race.

Between nuclear adversaries, distrust is especially strong, for very good reason, since each knows that the other can lay it waste. As a result, each side constructs so-called worst-case scenarios in which it imagines the enemy's most ingenious and devastating schemes, and then prepares to be capable of retaliating in kind—whether that be through ever more powerful nuclear weapons, through space weapons, or through the most inhumane chemical and biological weapons.

Each side does so in secret to the greatest degree possible, in order to foil the enemy. And because of their mutual secrecy, each suspects the other of far more treachery than meets the eye and prepares to respond in kind. In this way secrecy feeds on distrust

and nourishes it in turn. Together they increase international insecurity, propelling the arms race, making peace ever more fragile.

Surely the example of the secrecy of the Soviet military that led to the brutal shooting down last fall of the South Korean airliner was counterproductive even from the Soviet point of view, in addition to the tragedy it brought to the victims and their families. And the act itself led to increased world distrust and heightened tensions, spurring the arms race and undermining negotiations.

It is not only in our own strongest interest domestically to resist the immediate pressures for more secrecy. We also have urgent reasons to do what we can to reduce secrecy between nations. The United States, with its Freedom of Information Act and its society more open than most, has much experience to share in this respect. It has served as a beacon for peoples everywhere struggling with Government controls over what is spoken and written. We have a proud tradition to honor. There could not be a more dangerous time, domestically and internationally, to overturn this tradition.

Thank you very much.

Mr. KASTENMEIER. Thank you very much, Ms. Bok, for that eloquent testimony.

[The statement of Ms. Bok follows:]

Mr. Chairman and Members of the Subcommittee: My name is Sissela Bok. I teach philosophy at Harvard University and have written a book called "Secrets: On the Ethics of Concealment and Revelation". I am grateful for the opportunity to testify before your Committee; 1984 will be a year of decision with respect to government control over information in the United States. With its traditions of free speech and of a free press, and with its Freedom of Information Act and other restraints on official secrecy, the United States is hardly analogous to George Orwell's Oceania. But the pressures for more secrecy are strong, and never more so than when international tensions increase. The Administration, confronting in the Soviet Union a government that exercises pervasive secrecy and censorship, is now moving to reciprocate. It is as if it were trying to catch up in the secrecy race as strenuously as it pursues the arms race.

Those who have testified before this Committee earlier have spoken of the many different ways in which the government is pressing this secrecy race: through press censorship as in the invasion of Grenada, through measures to limit the Freedom of Information Act, and through expanded powers to classify information as Secret, as well as through limits on travel, research, publication and commerce in the private sector.

Perhaps the most dramatic and far-reaching of the new efforts to control information is to be found in the National Security Presidential Directive of March 11, 1983.

These many measures must be looked at together in order that their full force be grasped. They risk imposing direct government controls over what millions of Americans write and speak, not only in public service but in the private sector; and I believe that the indirect effects of such controls will be felt by all Americans.

Why should the United States, of all countries, with its traditional distrust of official secrecy, be moving in this direction? In a way the reasons are in one sense easy to understand. Faced with the extensive controls over information, travel, research and trade exercised by the Soviet Union and other countries, leaders of the Western democracies experience a dangerous imbalance, made all the more troubling now that the arms race and rising international tensions have so greatly increased the danger of armed conflict. In addition, the new technologies of intelligence—the methods of surveillance and photography, the satellites and the spy planes—have made all nations feel that their secrets are more vulnerable than ever.

While the motives are understandable, and I know your committee is taking them seriously, the drawbacks of tightening official secrecy should give pause. In the first place it has not been shown how the new measures will increase security. Just how will censorship in government and science, for instance, guard against the new technologies of surveillance? And even if such censorship could be enforced domestically, how would it avail against the flow of scientific and technological information, often of the highest order, between other countries?

As for leaking, does anybody really believe that lie detector tests will do much to arrest it? So long as high officials leak with impunity, others will follow suit; and at times leaks are of the highest importance to the public—as in the many revelations that exposed the Watergate abuses. Indeed, official secrecy and leaking exist in a symbiotic relationship; for as government secrecy expands, more public officials become privy to classified information and are faced with the choice of whether or not to leak; growing secrecy likewise causes reporters to press harder from the outside to uncover what is hidden. And then, in a vicious circle, the increased revelations give government leaders further reasons to press for still more secrecy.

Advocates of the stepped-up secrecy may agree that it is unlikely to do much for security, but conclude that nevertheless it is worthwhile even if it has only a limited effect—perhaps a “chilling effect” on at least some would-be leakers, for example, or a time lag before the public learns about military ventures abroad.

In so doing, however, these advocates often ignore or play down the second drawback of increased secrecy: the risks it carries for the nation which I believe are very serious. A look at secretive societies around the world shows that insofar as governments manage to impose official control over that is written, over research, over travel and public service, they undermine the most fundamental freedoms. The control, moreover, affects not only national security but, much more often, what would present a challenge to government leaders themselves: all that might prove embarrassing, all that stands in need of challenge, all that exposes failure and wrongdoing.

Now, political life in our country depends crucially on how the public perceives officeholders. They operate under the strongest pressures to avoid exposure of anything that would leave them open to criticism. It is folly to believe that the power to censor and control information would be restricted to legitimate national secrets. It never has and it never will.

To such warnings, proponents of tighter government controls might well retort that they intend to steer clear of all abuses of secrecy and all risks to the nation. But in the absence of explicit and adequate safeguards, this reply is entirely beside the point. No one, however well-intentioned, can know in advance how future American governments will use the secrecy and censorship provisions, once they are enacted. Nor can anyone guarantee that all those who exercise the new controls will be immune to the corrupting effects that secrecy—like all other exercises of power—can have.

The risks of secrecy are especially great when allied to unusual political or other power, and greatest of all when it is in the hands of government leaders. Because official secrecy allows governments to deceive and manipulate public opinion without any accountability whatsoever, it cuts at the very roots of democracy. It prevents citizens from perceiving and debating the issues, and often gives a false sense of their simplicity, suggesting that all is fine when it is not—as when our nation was misled by an elaborate system of secret double-entry book-keeping into ignoring the US bombardment of Cambodia during the Vietnam war.

The effect of the new measures on public debate would be devastating. Look back, for example, at the past month's Op. Ed. articles in a number of national newspapers written by former public officials, including such strong critics of present policies as Averell Harriman and Ambassador Robert White. How many would bother to write if they had to depend on advance clearance? And how many would receive it speedily enough for their comments to have timely impact?

Official secrecy and the silence and the manipulation it allows undercut what Simone Weil called “that interval of hesitation, wherein lies all our consideration for our brothers in humanity.” It is this interval of hesitation, of reflection, of timely debate, that permits citizens to think about what they owe to one another and to citizens of other nations.

Along with such risks to our democratic process, the new measures carry risks to the individuals on whom they are imposed. Scientists and others have already testified about their concern that censorship will dissuade some of the ablest among them from entering fields or undertaking research threatened by censorship. I predict that the same will happen with respect to persons in government service, already burdened by harassment and lowered income by comparison to past years. I base my prediction on conversations with both actual and prospective government employees. Their distaste for the new directive is striking, as is their sense of its adverse implications for their own lives and you can understand why.

Put yourselves in the place of someone wondering whether or not to seek government employment—perhaps for a few years only to begin with. Would you not think twice about accepting a position that would subject you to prepublication review for the rest of your life? Our country can ill afford losing the services of those with

enough independence and foresight to resist the thought of such lifetime censorship: those who think about their entire life and the restrictions that censorship would place upon it, and about the many different kinds of governments that this country may have in the future. If the new measures dissuade but a portion of able men and women from undertaking scientific research or going into top level government service, national security will be injured, not helped.

Given these threats to our democratic process, to individual liberties, and to national security from the new secrecy provisions, it is imperative that each one receive the most careful examination. And this must happen before, not after, they have taken hold; for alas it is much easier to institute such practices than to end them. We have to take seriously the claim that more secrecy is needed, but by itself the claim cannot suffice: we must be shown instances of the dangerous revelations thought to have harmed national security so severely as to subject the nation to the unprecedented new measures. So far as I know, advocates of the new regulations have produced no compelling set of such instances. Some have even argued that it would damage the nation's security interest to mention them at all. This will not do. Neither Congress nor the American public can be asked to accept the tightened secrecy on faith, without detailed demonstration of the evils it is supposed to remedy.

Only when the evidence is produced it will be possible to examine it critically. It will then be possible to consider just what dangers to national security are in question, and to ask how the stepped-up official control is meant to remedy them, whether it is likely to do so, what risks accompany each new measure, and what alternatives might better serve genuine national security.

In so doing, it will be important to consider yet a third reason to question the new secrecy measures—one that is international in scope. It concerns the role that secrecy plays in fueling the arms race. Every nation obviously needs a degree of secrecy for self-defense; yet most states use far more of it than is needed for purposes of defense. Throughout the world secrecy is a weapon in the hands of aggressors and an aid in every scheme of internal repression; and secrecy between nations has come to play a dominant role in increasing the distrust and suspicion that fan regional wars and propel the arms race.

Between nuclear adversaries, distrust is especially strong, for very good reason, since each knows that the other can lay it waste. As a result, each side constructs so-called "worst-case scenarios" in which it imagines the enemy's most ingenious and devastating schemes, and then prepares to be capable of retaliating schemes, and then prepares to be capable of retaliating in kind—whether that be through ever more powerful nuclear weapons, through space weapons, or through the most inhumane chemical and biological weapons. Each side does so in secret to the greatest degree possible, in order to foil the enemy. And because of their mutual secrecy, each suspects the other of far more treachery than meets the eye and prepares to respond in kind. In this way secrecy feeds on distrust and nourishes it in turn. Together they increase international insecurity, propelling the arms race, making peace ever more fragile.

Surely the example of the secrecy of the Soviet military that led to the brutal shooting down last fall of the South Korean airliner was counterproductive even from the Soviet point of view, in addition to the tragedy it brought to the victims and their families. And the act itself led to increased world distrust and heightened tensions, spurring the arms race and undermining negotiations.

It is not only in our own strongest interest domestically to resist the immediate pressures for more secrecy; we also have urgent reasons to do what we can to reduce secrecy between nations. The United States, with its Freedom of Information Act and its society more open than most, has much experience to share in this respect. It has served as a beacon for peoples everywhere struggling with government controls over what is spoken and written. We have a proud tradition to honor. There could not be a more dangerous time—domestically and internationally—to overturn this tradition.

Mr. KASTENMEIER. Your testimony speaks of the dangers posed by Government secrecy. You have also written of the value of secrecy or privacy for both individuals and society. What makes one form of secrecy good and the other evil?

Ms. Bok. Well, one element that is important there is the element of power. When Government controls secrecy, it has so much power over citizens that in a democracy this has to be dangerous.

A private citizen does not dispose of that kind of power. Moreover, personal dignity requires the protection of individual privacy in a way that is simply not analogous to the Government. The Government too has reasons for secrecy, but secrecy there has to be kept to a minimum.

We have to respect the exceptions, for instance, that are already in the Freedom of Information Act. We have to understand why those exceptions are there, but we do have to question every single new form of Government secrecy and that is simply not the case with respect to individuals.

Mr. KASTENMEIER. Incidentally, I noted that you copyrighted, or at least have given a copyright notice with your presentation. I do hope you will allow us to print it here.

Ms. BOK. Yes, I will. I give my permission. It is my custom to do these things.

Mr. KASTENMEIER. I yield to my colleague for a moment.

Mr. KINDNESS. Thank you very much, Ms. Bok, for your testimony.

I wonder if we might just examine your response to the chairman's inquiry a moment ago a little bit further, because I think that certainly I would start by saying that I agree with you very completely, I think, on the need for secrecy with respect to information relating to the individual, privacy considerations, and maintaining the dignity and freedom of the individual to dictate that there must be some secrecy available there.

But in a similar vein, there is a need perceived by some for dignity of a government as such, not only in international relations but domestically as well. It is a very dangerous concept, I think, but one with some validity. Drawing the line between enough and too much secrecy presents some very difficult problems and always has in our society, in the 20th century, at any rate, and probably always will.

First, might I ask, would you agree or disagree with the concept that there is a dignity factor with respect to governments that is appropriate to be considered?

Ms. Bok. Yes, I think you could use that in a metaphorical way, but I would say that the essential dignity of a democratic government really lies in the fact that it is a government by the people and for the people so that the dignity of a government has to reside in its openness and in its democracy.

However, I would add that there are reasons for secrecy in Government. And I would only say that the burden of proof should be very heavy upon the Government to show what those reasons are and why a particular measure is absolutely necessary in light of the democratic traditions and the commitment to citizens of openness.

Mr. KINDNESS. One of the facts that concerns me about dignity of government is that in international relations we are often viewed as being naive or silly or what have you by other nations, although they may respect our institutions and the openness of our society. It is fairly typical for Europeans and others around the world to view some of that openness as being excessive and perhaps causing us a degree of ineffectiveness as well as embarrassment in relations with other countries.

Do you believe that there is a ground for secrecy where negotiations are going on between the United States and another country which may or may not lead to an agreement of some sort?

Let's say it is arms limitation, or let's take it out of that area and put it in the area of trade, the dignity of position being negotiated. Is that a basis for warranting some degree of secrecy while those negotiations are going on?

Ms. Bok. Yes. I would definitely argue that there is, and I have in fact written about that in my book, *Secrets*.

Negotiations will very often fail if they are conducted in the open and so it is important to have a degree of secrecy there. However, even that secrecy should be limited to some extent.

It is obviously important to know who is negotiating with whom, with what country we are involved in the negotiations. And it is obviously important also to know at the end of the negotiations exactly what was agreed upon so that the Congress and the people have a chance to decide whether they go along, so that any secret clauses should not result from those secret negotiations. And there is always a danger with respect to secret negotiations that exactly that will happen.

There again, we do have to have some accountability. But I would definitely agree that some secrecy is needed for the process of negotiation itself, for the flexibility and creativity that would otherwise be destroyed.

Mr. KINDNESS. On page 7 of your written testimony, in the first full paragraph, second sentence, you refer to the unprecedented new measures. I take it you are referring there to the prepublication clearance and polygraph testing and that sort of thing that is involved in the Executive order.

I am confronted with a question of which comes first, the chicken or the egg. The existence of the Freedom of Information Act was new in its time, in a sense, and was therefore sort of unprecedented in that direction.

Ms. Bok. Yes.

Mr. KINDNESS. Since then, there have continued to be efforts to move back somewhere toward secrecy in various areas that may or may not be justified. But these unprecedented new measures presumably would not be proposed were it not for the literally unprecedented new measures represented by the Freedom of Information Act, as such.

Do we have a way to ever hope to draw a line and have an end to the settlement back and forth of these considerations? Do you think there is an answer, so to speak, for all time, or are we talking about something that will have to be constantly adjusted?

Ms. Bok. Well, first, I would just like to say that "unprecedented" is a word that one could obviously apply to everything including any word that one just says. I think both the pressure for secrecy and the pressure for openness that is manifested in the Freedom of Information Act have their precedents, in fact, in this country.

What is unprecedented in each case was the form that it took. With respect to these new measures, not only the institution of censorship for the first time in the United States but the combination of all those measures together are unprecedented.

The United States has had a lot of pressure back and forth over the 18th century and 19th century and 20th century with respect to secrecy, and I believe that that will have to continue. That should be part of our political process. But that process has to be conducted in the open and the public has to know what it is about, the new measures that are so necessary. That is why we have to have examples. We have not yet been given examples.

I think the debate about secrecy should always be conducted completely openly, even though we may agree at the end that certain kinds of Government information should remain secret.

Mr. KINDNESS. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. KASTENMEIER. I yield to the gentleman from Massachusetts.

Mr. FRANK. Let me just ask one question, which is, given the tradition in the United States, one of the problems I have with the effort that is now going on in the administration to impose all this secrecy is it seems to me even if you thought it was a terrific idea unlikely to be successful and that the effort to do it is going to produce a great deal of problems and not even accomplish the goal that it is seeking, given the nature of this country and the tradition you have been talking about, what is the likelihood of this kind of regime that they are talking about being imposed on people successfully?

Ms. BOK. Well, that I think is a very good question. I doubt that in this country, because of the tradition of people speaking out quite freely, speaking their minds freely, I doubt that this is going to work. I think that many of these measures will cause kind of an upheaval in this country that we may not have seen for a long time.

I really do believe that we could have new forms of civil disobedience by Government officials and others in the same way that we did have that about other important issues. I would say, for instance, that if the censorship provisions were to be applied not only to people who sign them now but to people who have been in the Government in the past and not signed them, then we would see former leaders of this country leading the effort of protest against those provisions and possibly refusing to sign, possibly being indicted.

So that is the greatness in a way of this Nation that it will take up issues like this and debate them to the fullest. And I do think that there will be a great deal of debate. But I would also say that trying to impose these measures could hurt the country.

I said before that it could hurt national security. Those people, for instance, who worked on the Manhattan project and who would not have even begun had they had to sign a censorship provision, are replicated in the 1980's by a great many others. So that the country will definitely be hurt, in my opinion, by the effort to impose the new measures.

On the other hand, I also think that that effort probably will not be immediately successful because it will arouse so much controversy.

Mr. FRANK. We could get the worst of both worlds.

Ms. BOK. I think we would.

Mr. FRANK. It seems that we are guilty of a quite unconservative failure to understand the limits of government and the strength of a nation's traditions.

I will yield back, Mr. Chairman.

Mr. KASTENMEIER. The gentlewoman from Colorado.

Mrs. SCHROEDER. Well, I, too, realize that the time is short and we thank you for being here. It has been a crazy, busy day.

I think the other thing that is important when you look at these new measures is that they are not directed against political employees. They are directed against civilian employees. If you look at many of the leaks, they have come from political employees and many of the civilian and professional people were never in the information loop to leak anyway.

So you have the harshness of the measure going into the group that really were not the offenders, which is very interesting.

Ms. BOK. Yes. I think that is important. And I do think that leaking by subordinates is not going to stop until it stops at the very top. If you are going to have measures for subordinates, then you should have them all the way up.

Mr. KASTENMEIER. On the point you made with respect to prepublication clearance, would it not be enough if we had such concepts as prepublication clearance but merely an affirmation by the agency that if the individual presumes to write a book after having left the Government, shall not reveal certain confidential secrets? That is to say, shall not reveal that which is classified any more than that individual would be enabled to do so with respect to communicating such secrets to any other person?

Ms. BOK. Yes, I think that would be enough. And, in fact, as I understand it, that is already the law in this country, that it is against the law to reveal classified information.

The trouble that officials often mention is that it is very hard to prosecute people for that, since they might have to reveal some other secrets in so doing. So then again you get into the secrecy problem.

Mr. KASTENMEIER. That is a law enforcement problem.

In any event, we are most pleased to have had you here today, Ms. Bok, and have the benefit of your views, your having written extensively on secrets, concealment, and revelation. Your books are well known in that area, and we appreciate your sharing your views with us on this committee.

Your testimony has concluded today's proceedings and this committee will be adjourned, although these hearings on 1984 civil liberties and the national security state and other questions relating to the area will be continuing in the near future.

Until that time, the committee stands adjourned.

[Whereupon, at 1:05 p.m., the subcommittee adjourned, subject to the call of the Chair.]

1984: CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE

THURSDAY, APRIL 5, 1984

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:40 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier, Glickman, Berman, and DeWine.

Staff present: Deborah Leavy, David W. Beier, counsel; Joseph V. Wolfe, associate counsel; and Audrey K. Marcus, clerical staff.

Mr. KASTENMEIER. The committee will come to order.

This morning the subcommittee continues with our fourth day of hearings on 1984 Civil Liberties and the National Security State.

Today, we will examine privacy protection in the computer age. The threat to personal privacy is a growing worry. A recent Harris poll showed more Americans, 48 percent, to be very concerned about this issue than ever before, and no wonder.

The same poll revealed four out of five believe it would be easy for someone to assemble a master file on their lives that violate their privacy. This hearing will consider whether that threat is real.

I would like to step back for a moment in order to gain some perspective. At the turn of the century, Americans had no drivers' licenses, no Social Security cards, no Selective Service registration. Only a few decades later, a small percentage paid income tax, and even fewer had passports.

All that, of course, has changed. Added to that web of information are, in recent decades, records generated by credit cards, credit reports, insurance claims, banks, and a host of other reasons to collect transactional information, personal data tracking, the transactions of modern life.

Ten years ago, the consensus developed that there was a need for Government intervention to protect such personal information. The Congress determined that Government should use such data only for the purpose for which it was collected, and that there should be no national data bank, no Big Brother computer.

Since the Privacy Act became law, there has been a tremendous increase in the collection of personal data in public and private sectors, data subject to increasing computerization.

This phenomenon leads us to the question: What are the dangers? Is the increase in personal data bases, combined with the capability of computers to interact with each other, plus the trend toward national identifiers, leading us to the creation of a national data center—an idea firmly rejected once by Congress.

The rapid advances of technology make it urgent that we in Congress reexamine the privacy protections provided by law to ensure that these defenses and personal freedom are not breached. We begin this task this morning.

Our first witness this morning has made our subject a major field for concentration. He is Robert Ellis Smith, publisher of the Privacy Journal, an independent monthly on privacy in the computer age.

Mr. Smith is also the author of *Privacy: How To Protect What's Left Of It* and *The Big Brother Book of Lists*; a former newspaper reporter, and he is also a lawyer.

Mr. Smith, I would like to greet you this morning. We have your statement and you may proceed as you wish, sir.

[The statement of Mr. Kastenmeier follows:]

STATEMENT OF ROBERT W. KASTENMEIER, CHAIRMAN, SUBCOMMITTEE ON COURTS,
CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE, APRIL 5, 1984

This morning the subcommittee continues with our fourth day of hearings of "1984: Civil Liberties and the National Security State". Today we will examine Privacy Protection in the Computer Age.

The threat to personal privacy is a growing worry: a recent Harris poll showed more Americans (48%) to be "very concerned" about this issue than ever before. And no wonder: this same poll revealed that four out of five believe that it would be easy for someone to assemble a master file on their lives that would violate their privacy. This hearing will consider whether that threat is real.

I'd like to step back for a moment in order to gain some perspective. At the turn of the century, Americans had no drivers' licenses, no social security cards, no selective service registration. A few decades later, only a small percentage paid income tax, and even fewer had passports. All that, of course, has changed. Added to that web of information are, in the recent decades, records generated by credit cards, credit reports, insurance claims, banks, and a host of other reasons to collect "transactional" information—personal data tracking the transactions of modern life.

Ten years ago, a consensus developed that there was a need for government intervention to protect such personal information. Congress determined that government should use such data only for the purpose for which it was collected, and that there should be no national data bank, no "Big-Brother" computer.

Since the Privacy Act became law, there has been a tremendous increase in the collection of personal data in the public and private sectors, data subject to increasing computerization.

This phenomenon leads us to question: What are the dangers? Is the increase in personal data bases, combined with the capability of computers to interact with each other, plus the trend toward national identifiers, leading us to the creation of a national data center, an idea firmly rejected by Congress?

The rapid advances of technology make it urgent that we in Congress reexamine the privacy protections provided by law to ensure that these defenses to personal freedom are not breached. We begin this task this morning.

TESTIMONY OF ROBERT ELLIS SMITH, PUBLISHER, PRIVACY
JOURNAL

Mr. SMITH. Thank you, Mr. Chairman.

I begin my statement this morning with a quotation from Alexander Solzhenitsyn, who indicates that as we give out the bits of information that you referred to throughout our daily lives, we really are creating what can best be described as a spider's web, a really vast network of information; some of it responsibly handled, some of it not so responsibly handled.

As Solzhenitsyn points out, we eventually develop a respect for those who control that information. And like any spider's web, it eventually can have the capacity to immobilize us.

I would like to today give an inventory of some of the data banks that now exist and also highlight what I think is a rather dangerous trend, namely, the Government is starting to learn that it doesn't have to gather the information itself, but can simply purchase it in the private sector. This has blurred the line between governmental action and commercial activity. Particularly it means the Government is relying on information collectors that have never had a strong reputation for accuracy or timeliness or responsibility in their information collection.

It is interesting to me, for instance, that the Government now is starting to rely on credit bureaus a good deal. On the other hand, the Federal Trade Commission, an arm of the Federal Government, has continually cited many of these same organizations for their sloppy recordkeeping. It is rather a strange irony.

On page 5 of my testimony there is a chart that indicates the sort of data that was collected in the fifties, the good old days, I guess. This was before computerization. The dotted lines on these charts indicate manual exchanges of information.

The credit bureau then was kind of a local mom-and-pop operation that was set up by the local department stores in town, not really tied into any other information collection throughout the community or Nation. That is not the situation at all today.

I don't think we can solely blame computers for the development. There were some simultaneous developments after the war. One was the increased reliance on insurance in our lives. Although many people had insurance during the mid part of this century, it wasn't as essential as it is to our lives now. Certainly, health insurance did not loom as large then.

Most retail purchases were not made on installment credit as they are now. Also, we were not as mobile a population; we stayed put. So that if you went into the department store and asked for credit, the merchants could rely on the fact that they knew your family, or they knew your roots. Now, by and large, in the marketplace, we deal as strangers; so that gives rise to the need for credit bureau-type operations.

It is also no secret that we had fewer transactions with the Government then in the fifties. That was an age when there was no Medicare and no Medicaid, no supplemental security income, no food stamps, very little student aid, no equal opportunity laws that required the collection of a lot of data. That all has changed, not only with the development of the computer but with some of these other trends.

Moving on now to chart 2, which is on page 7 of my testimony, you can see that the credit bureau has taken on much larger importance. It has become computerized. Because computerization re-

quired a lot of capitalization, a lot of large national firms bought up the credit bureaus in order to automate them. Most credit bureaus in the country now are owned by one of five large regional operations.

The credit bureau on this chart is the switchboard of the whole operation. It collects information from disparate sources and distributes it to other disparate sources.

Once again, the bold lines on chart 2 indicate computerized exchanges of information. You can see in the seventies that they were just starting to catch on.

You can also see that, by and large, they were confined to the commercial sector, the computer exchanges of information; very little between the Federal Government and the private sector at that point.

Let's move on now to the current situation with the next chart, chart 4, which indicates some of the new data exchanges in the 1980's. You can see now that the emphasis has shifted to the left of the chart with regard to mailing list companies now taking on a much larger role, and the Federal Government getting involved in all of this.

Just this month, the Office of Management and Budget is completing agreements that will permit any Federal agency to have 24-hour remote computer access to individual credit reports. The credit bureaus will be linked with the Federal agencies and have computer capability to process millions of transactional bits of information from banks, creditors, credit card companies, and retailers.

They also pick up information from courthouses around the country with regard to mortgages, liens, divorces, and lawsuits.

In turn, the credit bureaus will receive computerized information each month from the Federal agencies on individuals with Government loans, contracts, and grants.

Most shocking to me is that these organizations have never had a good reputation with regard to the accuracy of their information. I mention in my testimony some of the horror stories and the people who have been victimized by all this.

I should stress as we look at the chart, that it does not work as efficiently as it may look. This is really a Rube Goldberg device that we have created but there are lots of slips in the system.

The point is, however, that the technology now is in place for all of these exchanges, and many of them are going on. The most disturbing exchange is the one between credit bureaus and Federal agencies.

The next most disturbing one is the one between mailing list companies and the Internal Revenue Service. Now, the IRS has used mailing lists, at least on the regional level, for many years. What they are now proposing to do is use so-called demographic profile lists. These lists indicate the lifestyle of individuals. These are lists that computers create with the collection of information from disparate sources.

These so-called demographic lists would include people's purchases, their home ownership, their automobile ownership, the ethnic group that they belong to, the number of children; and also census information about their relative affluence.

These lists are precise enough for marketing products; but they are not precise enough for tax investigations at all. But that is what the IRS proposes.

This is a very good example of how the Federal Government is discovering that it doesn't have to gather the information itself and follow all those procedural safeguards of the Privacy Act, but that it can buy the information in the marketplace.

Another disturbing trend is that the Department of Treasury is proposing that direct deposit of payroll checks be mandatory for all 2.8 million Federal employees. I think an individual ought to have a right to choose a depository institution and not have to report that to the Government; and should have the right not to have a depository institution.

I also think, and there is some evidence of this, that once the Federal Government institutes this mandatory direct deposit, the private sector will follow suit.

I had a call from a person in Orlando, FL, who told me that his company wanted him to authorize withdrawal of his account as well as deposit in case there was some overpayment by error.

What this means is that we will be seeing many more exchanges of personal data between another large government agency, the Department of Treasury, and the Nation's banks.

There has been testimony in the Congress about computer match procedures instituted by the Federal Government for about the past 3 or 4 years. It is extremely controversial.

Many matches create a general search of the kind that the framers of the fourth amendment intended to ban. Matches are in fact governmental actions generally searching one's papers and one's effects.

A few States have access to individual bank account information. Massachusetts, for instance, requires that all banks match Social Security numbers with lists of welfare recipients to see which recipients may have savings accounts over the allowable limit. Most State welfare departments now exchange data with private employers and with public employers to determine who may be on a payroll and receiving income over the allowable limit.

These exchanges don't always work as efficiently as they look on paper. For instance, many matches might involve looking at the payroll records of February, compared to the welfare rolls of March. If somebody turns up on both lists, a so-called hit, he or she may be on both lists legitimately. There have been lots of problems with that. People get knocked off the rolls and then they have the burden of showing that they in fact belong on the public assistance rolls.

The Treasury Department, in trying to restrict travel to Cuba, which has been done for many, many years, is now not looking at the passport as the main means of control of travel outside the United States to a particular country; but the Department has discovered a fact of life: you look to the credit card companies for a way to maintain surveillance.

The Treasury Department, in fact, is not prohibiting travel to Cuba. It is prohibiting the use of plastic in Cuba—and it proposes monitoring private credit card companies in order to see who has been trying to use credit in Cuba. That scheme has been enjoined

by the First Circuit Court of Appeals. The case is now before the U.S. Supreme Court, *Regan v. Wald*, No. 83-436.

Just parenthetically, the travel offices of most Federal agencies have direct computer access to airline reservation systems. I am not sure of all the implications of that, but I point it out as a computer exchange that may have started off very innocently but may have some rather ominous overtones.

Just about all State motor vehicle departments disclose auto registration and driver license information by computer to Dataflo Systems, which is a Division of Equifax, formerly known as Retail Credit Co. To complicate matters, Equifax is the owner of one of the largest credit bureau operations in the Nation, including the Credit Bureau here in Washington which has files on probably just about everybody in this room.

Equifax also is the largest consumer investigating company in the Nation, which collects information from neighbors and from employers, for purposes of insurance applications and insurance claims.

In fact, many motor vehicle departments rely on the private sector to keep their records straight and go, in fact, to places like Dataflo and Donnelly Corp. in order to get the information that they need out of their own records.

Congress has authorized, in the last several years, several more exchanges of data between the public sector and the private sector. The food stamp program, Veterans' Administration, Housing and Urban Development, Health and Human Services, and Labor, have access to computerized payroll data in the private sector.

There are also some disturbing exchanges of personal information within the Federal Government itself. In my testimony, I point out three. First, Selective Service, which has compiled probably the most efficient data bank in town, because it is a felony if you don't keep it up to date. It is a crime not to report to the Selective Service your latest whereabouts.

It is a known universe of young men between certain ages, and I think every Federal interagency in town wants to get its hands on that data bank. It is now made available to the Parent Locator Service, which tracks down people who are not keeping up support payments, and has been made available to the Internal Revenue Service and to military recruiters as well.

I think this is a breach of an understanding made with the young men who signed up for Selective Service. They were led to believe that they were to be on file in case they were needed for draft purposes because of a national emergency. In fact, now it is "open season" on these records for other purposes: tracking down child support, and the Internal Revenue Service, military recruiters, and I am sure others will now want to start getting into that system.

We have a law on the books that requires registration with the draft in order to qualify for Federal aid. I presume that in order to monitor compliance with that act, there will be some sort of automated exchange of information before long between Selective Service and the Nation's universities.

In addition, Federal agencies are now authorized to get from the IRS addresses and back taxes owed by loan applicants.

It was interesting to me to discover, not surprisingly, that when you start to use Internal Revenue Service records for other purposes, people start to be less candid with their government. The Internal Revenue Service noticed that when you start having a scheme to withhold from people's refund checks any child support that they owe, it is not surprising that the next year these people are not going to have as much money withheld from their payroll. That in fact is what has happened.

So, although the Government is tracking down child support payments, it in fact is losing out on a large amount of the float that it enjoys by excessive withholding. That, we should have anticipated.

The key to a lot of this linkage is a social security number. And the current legislation on the books really is inadequate to address this problem. The leading complaint I get from readers and others in my work is that they really don't have a sense they can do anything about demands for their social security number. Just about everybody wants it, including the private sector as well as the public sector; and the Privacy Act affords only very slight protection with regard to governmental agencies and totally excludes State welfare, tax, and motor vehicle departments.

On the charts that I have shown here, just about all the agencies indicated have social security numbers except for most mailing list companies, many utilities, the testing services, and cable television systems.

The Medical Information Bureau, which is on the right of the chart, keeps records on more than 11 million citizens without the Social Security number; so it shows that it can be done.

Social Security numbers are an important symbol of people who are resisting invasions of privacy and, as I say, it is also the one means by which data can be linked.

It is worthwhile for the Congress to take another look at that and to have some protection for citizens who choose not to provide their Social Security number to, for instance, the cable television system, or a department store with which they are doing business. Currently there are no such protections.

Chart 5 in my testimony indicates the legal protections, such as they are; the dotted lines indicate some partial protections. Credit bureaus and consumer investigators are pretty well covered by the Fair Credit Reporting Act of 1971. Federal agencies are covered by the Privacy Act of 1974.

A lot of citizens probably think that the Privacy Act provides them some coverage beyond that, but it applies only to Federal agencies. It has some loopholes in it because it permits some computer matching of information, which I think violates one of the principles of fair information practices, namely, that information gathered for one purpose ought not to be used for another purpose. But there have been justifications within the Federal agencies that say that to have such matches does not violate the Privacy Act.

Federally supported school systems and universities are covered by the so-called Buckley amendment, the Family Educational Rights and Privacy Act of 1974. The Tax Reform Act of 1976, and also the Financial Right to Privacy Act prohibit Federal investigators from having access to bank records without some procedural

safeguards. But there are no prohibitions against local investigators, or private investigators from having access to bank records.

Many people think that their bank records are secure, and that isn't the case. More so with regard to medical records—most people think that there is confidentiality of medical information in this country. They are confusing that with a privilege, which means that a physician is not required to testify about medical information that he receives. But there are very few laws that say a physician can't voluntarily release information, and that is done frequently; and, of course, physicians are exchanging information with insurance companies all the time.

Also, the privilege only pertains to a court proceeding. So, there are very few prohibitions against the disclosure of medical information; by the same token, very few rights of access to medical information. You don't have the right in this country as a matter of law, except in a few States, to even see your own medical file.

In the chart of the 1950's, you notice that the hospitals and M.D.s were off in a corner with no real linkage to the rest of this spider's web. You see in some of the later charts that they are now very much tied into it. What used to be a one-to-one relationship with your doctor, now involves a triangle; it is a triangle among the health provider, the health insurer who is paying the bills, and your employer, because most health insurance is administered where you work. The person left out of that triangle is the patient. The patient does not have access to that information that he has to authorize others to see. I think that is an injustice that ought to be addressed; maybe three or four States have done it. A bill that would provide some protection came very close to passage in 1980.

I have touched on two areas. Another growing area is interactive cable television. There is some dispute in the industry as to whether it is really going to catch on and whether people are really going to want to buy products over cable systems. But if it does catch on, it will concentrate an awful lot of very sensitive personal information about people; information that I think is just too juicy for commercial interests to keep their hands off. And only four States, including your own State of Wisconsin, by the way, have protection with regard to cable television systems.

S. 66 in the Senate does provide some procedural safeguards with regard to that. I think it is an area that both Congress and State legislators ought to look into.

There is no right of an employee to see his own personnel file except in 10 States. Once again, Wisconsin does have that protection. I think that ought to be nationwide. I think that is just elementary, that people ought to have a right to see their own personnel file and their own medical file.

I think there ought to be limits on computer matching. Generally the executive branch has gone on with computer matching without much restriction by the legislature and I think that many of these matches, when they involve disparate data banks, do violate the fourth amendment.

We ought to find ways to erect barriers between the private and the public sectors to prevent the wholesale exchange of personal information without guidelines and without precautions.

Lastly, all of this has to be overseen in some way. It is disturbing to report that this administration is the first, since 1973, when we first had that revival of interest in privacy, not to have any one contact point in the Government, in the White House, with regard to privacy. Each White House since the Nixon administration, including the Nixon administration, has had some component within the White House that looked after privacy, data collection, and surveillance matters.

The Office of Management and Budget has a very narrow jurisdiction with regard to the Privacy Act and hearings in other committees have shown that they are not really exercising that jurisdiction to the full extent that they should.

Most European nations have a privacy ombudsman that can handle complaints, can resolve some of these things. An awful lot of these complaints perhaps are addressed better not by legislation, but by some sort of complaint mechanism, and some sort of ombudsman or at least a clearinghouse for people to go to in the Federal apparatus.

One final point, with the European nations passing laws now that limit the export of information, they are saying that a company in Europe cannot export data back to the United States unless that country receiving the information has data protection as strong as the European nations.

Our data protection is rather spotty, as you can see from the chart; so many companies are finding that because we don't have stronger protections here in the United States, that export of personal data back to the United States for computer processing will be prohibited.

Also, we have no strong representation of U.S. interests on this matter in these European circles where data protection is very much a live issue.

That concludes my testimony, Mr. Chairman. I hope I have scared everybody sufficiently, and I would be happy to answer your questions.

[The statement of Mr. Smith follows:]

STATEMENT OF ROBERT ELLIS SMITH, PUBLISHER, PRIVACY JOURNAL, WASHINGTON, DC, ON "1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE"

As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands—buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

ALEXANDER SOLZHENITSYN, *Cancer Ward*.

Many people in America think that all personal information about them is stored in one central, all-knowing computer somewhere, perhaps under a mountain west of Washington; many others think that the various institutions with which they deal gather specific information for a particular purpose and then keep it responsibly under lock-and-key. In fact, computerized information collection in the 1980s more resembles a huge web, in Alexander Solzhenitsyn's metaphor, a great complex of responsible and irresponsible data-gatherers, some of them regulated by record-keeping statutes, most of them not. A few of these data custodians have traditions of

respect for confidentiality and accuracy, but most do not. A few train their personnel in responsible data collection and treat personal data as if it were held in trust, but most do not.

This series of hearings on "1984: Civil Liberties and the National Security State" is an appropriate time to take an inventory of these diverse data banks and their interrelationships. It is an appropriate time to identify a disturbing trend of the mid-1980s: government agencies are more and more relying on the private sector to provide sensitive personal individual information about American citizens, instead of gathering the information themselves. This threatens individual privacy by diminishing the control individuals have over information about themselves. It also means that the government is relying on several data gathering outfits that are notorious for their sloppy information collection. (The two largest credit-bureau networks, the largest consumer reporting agency, the trade association of credit bureaus, and the clearinghouse of medical information for 700 insurance companies have all been cited by entities of the federal government for inadequate handling of personal information. Yet the federal government itself has become a large customer of these organizations.) This further means that the crucial demarcation between governmental action, in which there is constitutional protection for citizens, and commercial activity, where there are no such protections, has become irretrievably blurred. This increased linkage of government and non-government data collection tends to diminish the quality of information in each sector, because applicants start falsifying information, or withholding it, when they fear that information that they provide will sooner or later be used for a purpose other than the one for which it was collected.

THE FIFTIES

The Fifties were a time when only the Bureau of Census and the Social Security Administration had any real capacity for automated processing of personal information. Storing personal data was awkward (and expensive). Merging records with those in other data banks was impossible. Manual files took up a lot of physical space, and they had to be purged periodically. In the Fifties all of the computers in use in the U.S. could be placed in a space the size of the Capitol.

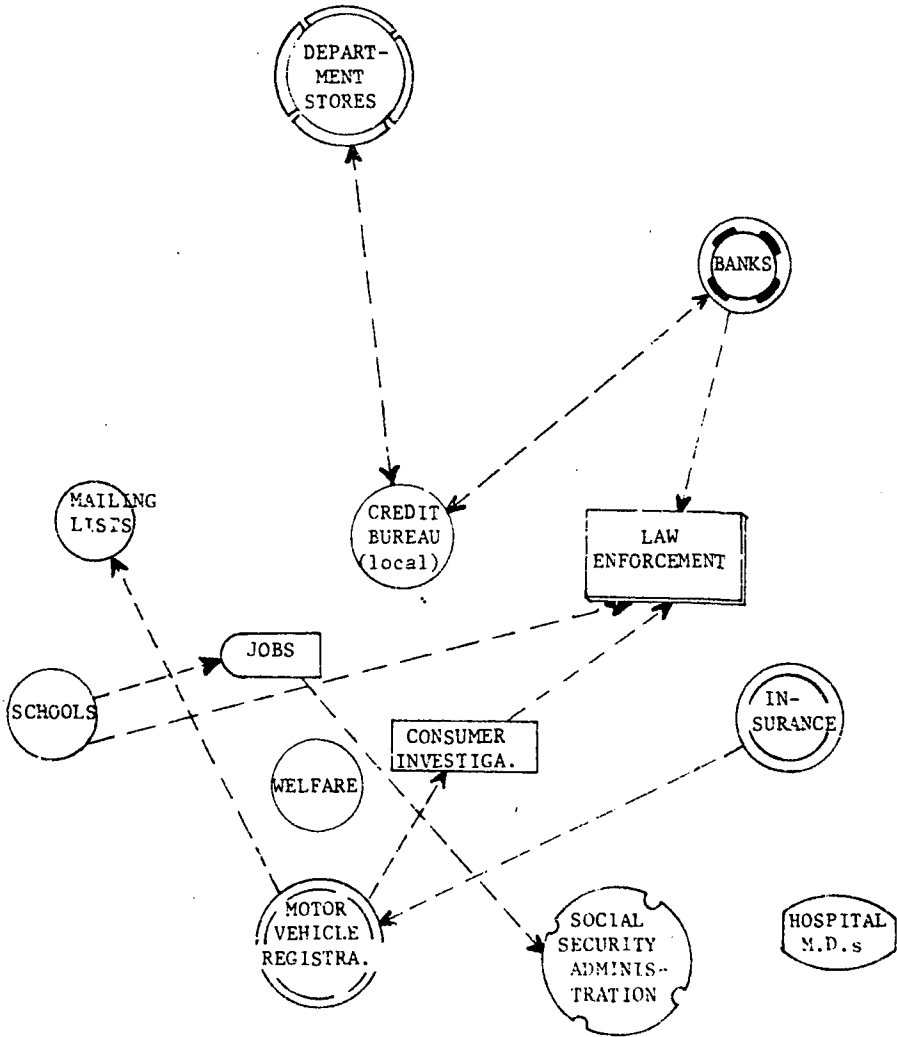
It is remarkable that, despite the proliferation of data banks in the past two decades (see Chart Two), that same fact is probably still valid. All of the computers in use in the U.S. in the 1980s could fit within the same space within the U.S. Capitol. This is true because of the miniaturization of the technology. Thus, in the 1980s, the major deterrents to massive data gathering have virtually disappeared—space, cost, difficulty of access, and vulnerability to fire or other damage.

There were other factors in the 1950s, besides the lack of computerization, that meant that information collection was not a large threat to personal privacy. Insurance was not a dominating factor in our lives. Most states did not require auto coverage, and the majority of health-care bills were paid by the patient, not, as today, when 90 percent of health-care bills are paid by a "third-party payor," whether a private insurance company or the government. Fewer purchases were made on credit then, and so retailers did not need personal information to predict credit-worthiness. In the 1950s about eight percent of the average family's budget was spent on installment credit; now the figure has doubled. More than half of all retail purchases are now made on credit. There were very few credit cards in circulation three decades ago, only those issued by oil companies and retail stores. No travel-and-entertainment cards; no bank cards. Now nearly 100 million Americans have credit cards, an average of six per person.

Even if merchants in the 1950s had to make credit checks, they could do so informally at the local level. We were not then such a mobile population. In the 1980s about half of us do not live in the hometowns where we were raised; we are strangers to the institutions from which we expect credit. This has given rise to large, regional credit bureaus that rely totally on computerization and telecommunications. In addition, in the Fifties, the average person had few transactions with government agencies; there was no need to provide the government with much information about ourselves. No Medicaid and Medicare, no OASHA, no equal opportunity laws, no student aid, no Supplemental Security income, no food stamps, no complicated tax deductions that require the giving up of personal information.

Information exchanges among private and public institutions in the 1950s are illustrated in Chart One.

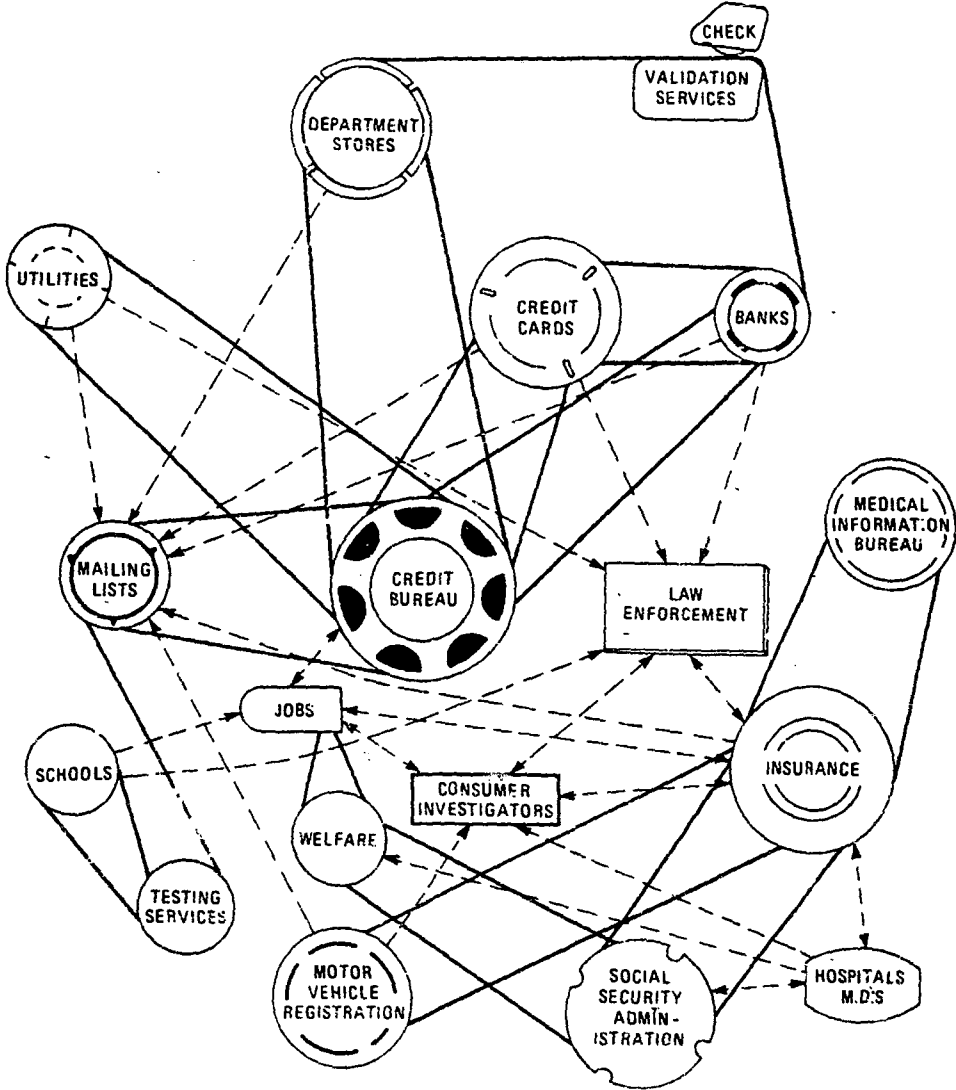
Chart 1



THE SIXTIES AND SEVENTIES

In the 1960s came a proposal for a Federal Data Center that would have consolidated personal data collected by federal agencies. There was great popular and political opposition, leading to increased concern about privacy. The 1970s brought a succession of federal and state laws providing some protections. It could be said in that decade that just about every salient fact about a person was on file somewhere, and most likely on file in a computer system; but it could also be said that hardly any of these computer data banks were connected with each other. There were few if any links of data between the federal government and the private sector. The Privacy Act of 1974 discouraged exchanges of data between and among federal agencies and between federal agencies and non-governmental institutions. The extent of exchanges among data banks in the late 1970s is represented by Chart Two. Each solid line represents an automated exchange of information between the two agencies. The arrows show the direction of the information flow; sometimes it is one-way, sometimes it flows in two directions. The broken lines represent manual exchanges of information.

Chart 2



THE EIGHTIES

In the 1980s, it must be said that there is an inexorable trend in the direction of linkage. Here are some examples:

1. This month, the Office of Management and Budget will complete agreements that will permit any federal agency that wants it to have 24-hour remote computer access to individual credit reports stored by seven different companies. The credit bureaus to be linked with federal agencies have the computer capability to process millions of transactional bits of information from banks, creditors, credit-card companies, and retailers. They also pick up information from courthouses around the country pertaining to mortgages, liens, divorces, and lawsuits. In turn, the credit bureaus will receive computerized information each month from the federal agencies on individuals with government loans, contracts, or grants.

The most shocking aspect of this exchange authorized by Congress is that the credit-bureau has a poor reputation for maintaining the accuracy of its information. The most sophisticated company in the business, TRW Information Services, estimates that of the approximately one million persons who ask to see their files each year (as permitted by the Fair Credit Reporting Act), fully one-third challenge the information they see in the files. Another of the top five companies, Trans Union Credit Information, regularly mixed up a person's credit report with that of a son, or daughter or parent, or even with a person of similar name living in a different city, according to the Federal Trade Commission in 1983. TRW continued to report erroneous delinquencies from two Michigan department stores after a consumer "fervently complained," according to the Sixth Circuit Court of Appeals. A credit bureau in Maryland erroneously implied that a Vietnam veteran had been dishonorably discharged. A San Antonio credit bureau refused to correct an erroneous bad debt that should have been placed in the file of another man with a similar name. A check guarantee company in Kansas City negligently black-listed a man who "had never written a bad check in his life," according to the Court of Appeals in Kansas in 1981. When a Cleveland man demanded the file maintained on him by Equifax Services Inc., he saw that it contained erroneous gossip and was barely literate. Equifax has also included in its files the fact that a person has filed a legitimate complaint with the Occupational Safety and Health Administration. Many credit bureaus have been plagued by dishonest employees who alter credit reports for a fee. Federal agencies should not be using these dubious files, nor adding information to them.

2. The Department of Treasury is proposing that all 2.8 million federal employees must agree to direct deposit of their pay in order to keep their jobs. This will vastly expand the current electronic exchange of personal data between the Department of Treasury and the nation's banks, savings and loan associations, and credit unions. Already a third of all Social Security payments and half of the federal payroll are electronically transmitted directly to the recipient's financial institution. Mandatory direct deposit will mean that a federal employee must use a depository institution and must reveal its identity to the government. Private employers are sure to follow this federal policy, and some already have. Some private employers even ask employees to authorize direct withdrawal from personal accounts, as well as direct deposits (in case of overpayment by error).

3. To administer its Basic Educational Opportunity Grants, the Department of Education has access to sensitive parental financial disclosure forms filed with the College Scholarship Service, owned and operated by the private Educational Testing Service in Princeton, NJ. (One of the service's requirements is that parents agree to permit access to individual tax returns if the scholarship service so requests.)

4. The Internal Revenue Service is now renting computerized lists that provide "demographic profiles" of various households. These "lifestyle" lists include the following information on those listed: name and age of each family member, recent purchases, religion, ethnic group, telephone number, approximate income, length of residence and dwelling size, children's birthday, Census tract, and postal carrier. Similar lists reveal magazine subscriptions, catalog purchases, auto ownership, charitable contributions, and political party affiliation. The IRS is not merely using the lists to determine who is not filing tax returns (it has rented conventional mailing lists for years to do this, and no one quarrels with this). IRS is using these "lifestyle" lists to determine whether individual taxpayers are filing returns that reflect a consumer lifestyle that is portrayed in these demographic lists. This is unfair because the lists are based on cumulative data that are not precise enough for individual enforcement investigations and because the information was provided for a

Available Data on 35,000,000 Families. There is no other source that can provide either this level of specific information, or level of reliability.

D-S-I. FAMILY HISTORY
 MR ROBERT CORRICK
 88 SIMPSON CIR
 AGAWAM, MA 01001

NAME	YOB	SEX
CHILD 1 GERALD	LC	H
CHILD 2 CATHLEEN	LP	F
CHILD 3 LORI	67	F

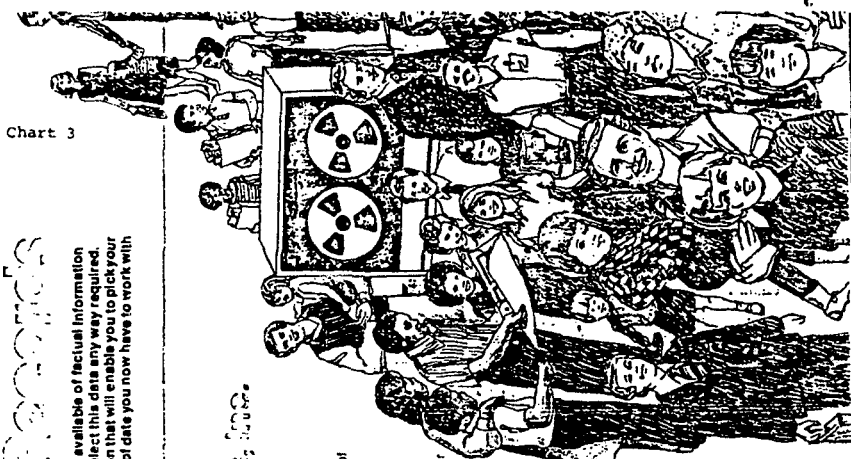
DWELLING-SIZE C* LOR 11**
 ART-SPENT \$15
 TELEPHONE 765-6621*

*NOT AVAILABLE ON ALL HOUSEHOLDS

INFORMATION FIELD DESCRIPTION

- TITLE
- SEX
- First Name of Adult Head of Household
- Family Surname
- House Number
- Street Name
- Response Date
- Birth's Age
- No. of Purchases
- Media of Response
- Type of Purchase
- Religious Code
- Carrier/Non Carrier
- Post Office
- Telephone #
- Home Tract Median
- Dwelling Unit Size
- Length
- Residence
- City Name
- State Abbreviation
- Zip Code
- 1st Child's First Name or Initial
- 1st Child's Age
- By Year of Birth
- 1st Child's Sex
- 2nd Child's First Name or Initial
- 2nd Child's Age
- By Year of Birth
- 2nd Child's Sex
- 3rd Child's First Name or Initial
- 3rd Child's Age
- By Year of Birth
- 3rd Child's Sex
- Month of Birth
- Gender
- Race
- Family Record Number

Chart 3



Demographic Systems Inc. maintains the largest file available of factual information about families, their members and future, and can select this data any way required. 35,000,000 families identified with specific information that will enable you to pick your universe quickly and economically. Check the depth of data you now have to work with to solve many of your research requirements.

- Adults by name, and year of birth
- Children by name, and year of birth
- Family size
- Family members' ages
- Male headed households
- Female headed households
- Working women by age
- Families by income
- Families by religion
- Families by type of home
- Pre-School Children (Under 5 years old)
- Grade School Children (6 to 12 years old)
- High School Children (13 to 18 years old)
- Young adults (19 to 21 years old)
- Families with 2 children
- Families with 3 or more children
- Parents of children (by age of child)
- Apartment families with children
- Home owners with children
- Adults (22 to 34 by year of birth)
- Adults (35 to 49 by year of birth)
- Seniors: Citizens (over 50 years of age by year of birth)
- Single females (by age)
- Married females (by year of birth)
- Married males (by year of birth)
- Individuals by month of birth
- Telephone subscribers
- By year of birth
- New homeowners (3 months after move)

5. Under "computer match" programs pushed by the federal government, state welfare departments have access to batches of payroll data from private employers, to determine which welfare recipients also show up on lists of persons earning money in excess of the allowable limit. A few states have access to individual bank account information, for purposes of computer matches by welfare departments, to determine which recipients have savings assets above the allowable limit.

6. To restrict travel to Cuba, the Treasury Department is attempting to monitor periodically activity in accounts maintained by private credit card companies. (The First Circuit Court of Appeals has enjoined this scheme.)

7. The travel offices of some federal agencies, the military, and many overseas embassies have computerized access to airline reservation systems, much like travel agents. These systems include data on the comings and goings of millions of persons (although there is no access by passenger name without more specific information about flight schedule, and there are supposed to be limits on the access that is possible for each travel office).

8. Just about all state motor vehicle departments disclose auto-registration and driver-license information, by computer, to Dataflo Systems, a division of Equifax Inc. (formerly Retail Credit Co.), which in turn supplies it to inquiring insurance companies. This data includes, Social Security number and permit number, date of birth, physical description, type of permit and restrictions, and a list of violations. Many states provide this computerized information to compilers of city directories. The average state releases masses of motor vehicle information to attorneys, fund-raising organizations, individual insurance companies, auto manufacturers, mailing list brokers and compilers, catalog publishers, law enforcement agencies, and political campaigns, according to a report issued by the Secretary of State in Illinois in 1983.

9. Federal agencies, including the Food Stamp program, Veterans Administration, Housing and Urban Development, Health and Human Services, and Labor have access to computerized payroll data from private employers.

10. Private insurance companies like Aetna, Mutual of Omaha, and Blue Cross-Blue Shield, as Medicare "intermediaries" processing payments for the government, have computer terminals with access to the massive Social Security Administration Data Acquisition and Response System (SSADARS). Other agencies with on-line access include the Internal Revenue Service, the Departments of Agriculture, Labor, and Health and Human Services, state public assistance agencies, food stamp offices, and the Railroad Retirement Board. The system includes data on retirement, disability, Supplemental Security Income (SSI), and Medicare benefits, but private insurance companies are supposed to have limited access to only part of the data base.

11. The Department of Education, the Veterans Administration, and every other federal agency (under the Debt Collection Act of 1982) provide information on debtors in federal programs to private debt collection agencies and consumer reporting agencies and in turn receive back information.

There are disturbing exchanges of personal information within the federal bureaucracy, as well:

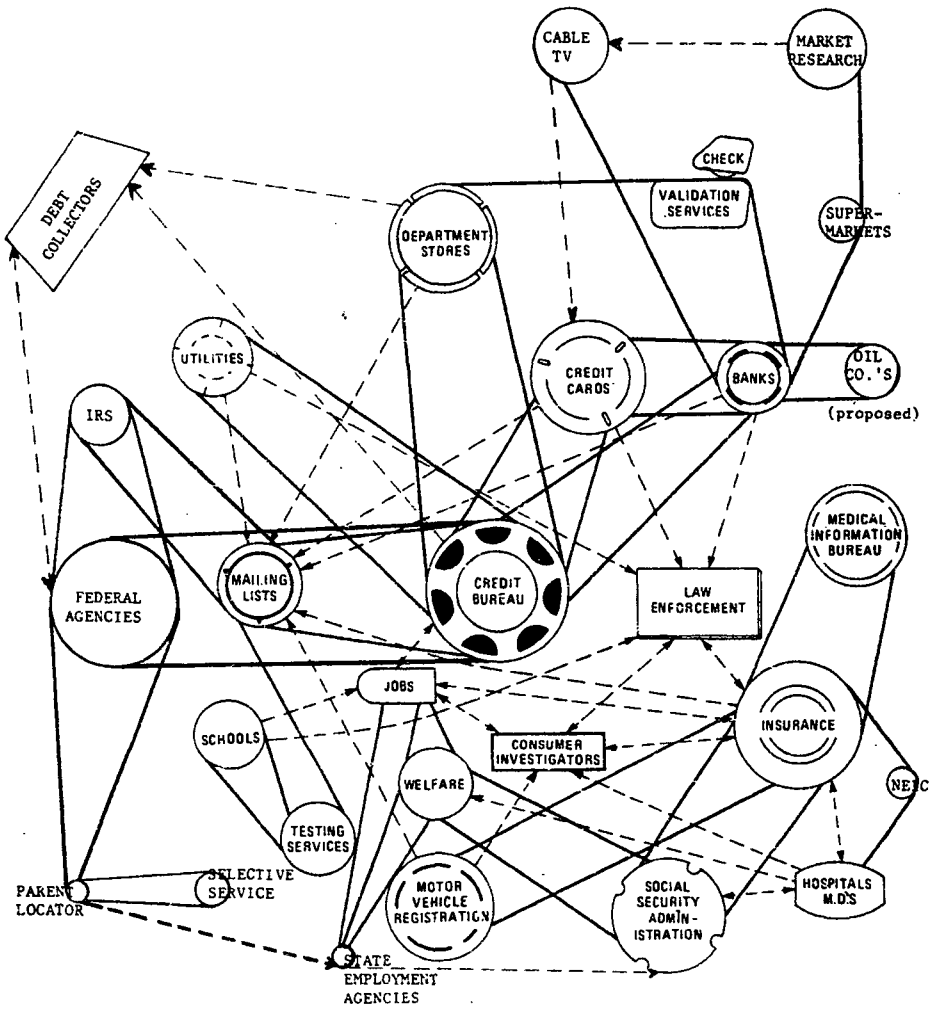
1. The Selective Service System makes its lists of young men available to military recruiters, to the Parent Locator Service, and to the Internal Revenue Service. This violates the principle that information provided for one purpose ought not be used for a second purpose without the consent of the individual. In turn, the System has had access to driver records in 49 state motor vehicle departments, as well as limited use of IRS records, Veterans Administration files, and Social Security files.

2. The Parent Locator has access to all federal agency records except the Bureau of Census. By law, the Internal Revenue receives information from the Parent Locator Service and deducts from tax-refund checks any amounts said to be owed by a taxpayer for child support. (The IRS has discovered that one-fourth of those subjected to this withholding of refunds in 1981 did not file tax returns in 1982. Two out of three of them significantly reduced the amount of taxes withheld from their pay by their employers—thus contributing to a significant reduction in the amount of free float the federal government enjoys in surplus withholding.)

3. Federal agencies are now authorized to get from the IRS addresses and back taxes owed by loan applicants.

The current exchanges between and among private and public organizations in the mid-1980s are represented in Chart Four. What had been essentially two separate networks, one private and one federal, is becoming merged into one. (NEIC on the chart is the National Electronic Information Corp., a computer system that processes insurance claims from hospitals and other health-care providers and directs them to one of several major insurance companies.)

Chart 4



© 1984 Robert Ellis Smith

SOCIAL SECURITY NUMBERS

The key to these linkages, of course, is the Social Security number. Of the agencies represented in Chart Four, only a few do not include SSN in their data bases. Those without the SSN include the Medical Information Bureau, secondary school systems (most of them), most mailing lists, many utilities, testing services (generally), and cable television systems. This linkage by way of the SSN is one reason why many people resist providing their Social Security numbers to any agency that asks. Yet there is no law that provides these aware citizens any protection. In fact, in many states, the number is displayed on one's drivers' permit. It is also readily available from a credit bureau to any institutional subscriber that asks.

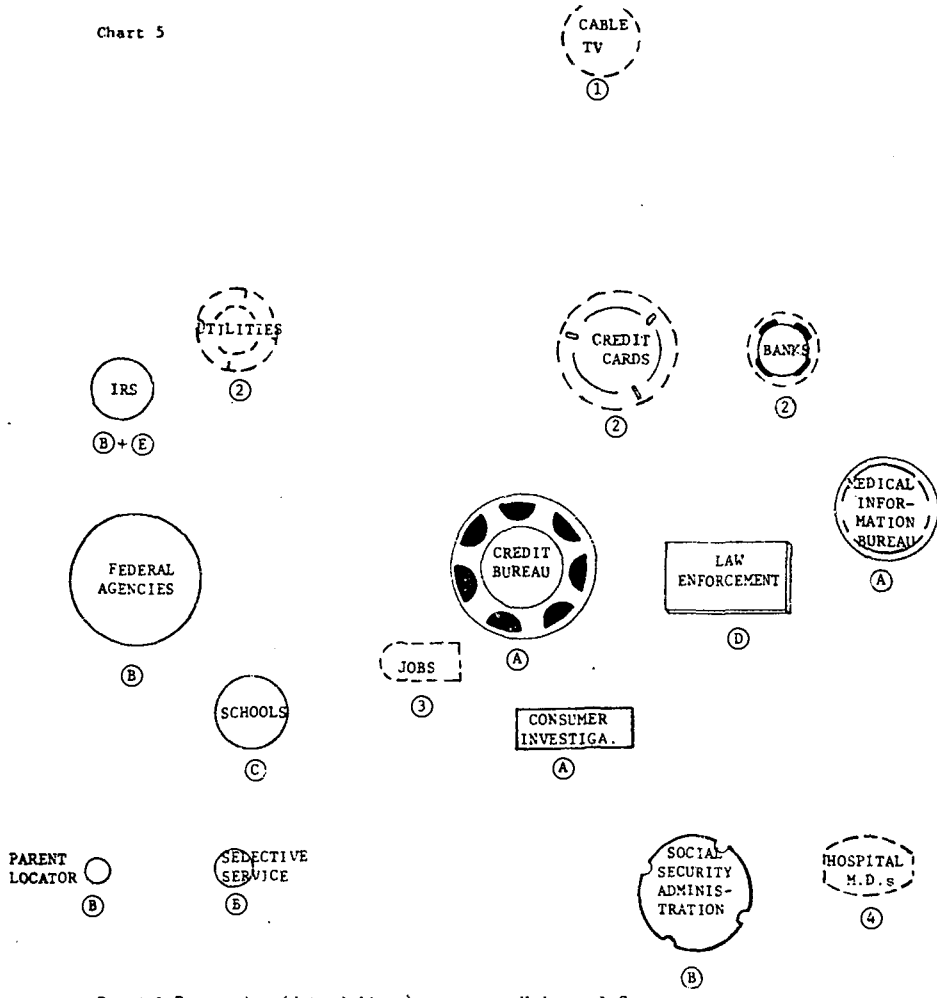
The Social Security number is an imperfect identifier. Some people have none, some people have more than one, and still others share the same number (often without realizing it). People are rarely totally careful when providing the number on an application form and agencies rarely bother to check it, because providing the transaction is rarely affected by the accuracy of the number. Yet, in a computerized match, that number takes on larger significance, because it is generally the one data element on which a "hit" is based. Thus, a bit of data about each person that is casually provided and still more casually stored becomes crucial in determining whether an individual comes under suspicion for fraud.

The Privacy Act of 1974 as amended (5 U.S.C. 522a note) limits (but does not prohibit) demands for the Social Security number by federal, state, and local government agencies (except for state motor vehicle, welfare, and tax departments) unless there was a law or regulation on the books prior to 1974 authorizing such demands. Further, financial institutions are required to have a taxpayer identification number on each account holder (31 CFR 103.34).

LEGAL PROTECTION

Chart Five indicates the data-collection agencies that are covered by federal laws. The federal laws limit disclosure of personnel information, permit an individual an opportunity to inspect and challenge information in a file, and obligate the data gathering to keep information accurate and timely. An exception is the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401), which provides some procedural safeguards when federal investigators want access to "third-party" financial and credit information held by banks, credit card companies, and telephone companies. Only a few states have limits on what a bank can disclose to state, local, or private investigators, or to commercial companies.

Chart 5



Partial Protection (dotted lines)

- (1) Four states, D.C. limit disclosure of subscriber information.
- (2) Financial Right to Privacy Act limits outside access.
- (3) Nine states permit public or private employees to see personnel files.
- (4) 12 states permit patients access to own files; few if any limit disclosure to outsiders.

Universal Coverage

- (A) Fair Credit Reporting Act.
- (B) Privacy Act of 1974.
- (C) Family Educational Rights and Privacy Act of 1974.
- (D) Federally funded criminal justice systems provide right of access and correction, as do many state laws.
- (E) Tax Reform Act of 1976 provides confidentiality IRS, with exceptions.

NEEDED PROTECTIONS

Clearly there are some gaps in the legal protections, and these deserve attention by the Congress and state legislators.

1. First there should be limits on demands for the Social Security number, mainly in the private sector, unless the number is needed for tax-reporting purposes.

2. The growing area of interactive cable television (and allied technologies that provide text material on the screen) deserves scrutiny. It may be that these interactive services will not be a big hit among consumers; but if they are, there will be a significant concentration of sensitive personal information stored by cable companies—a family's choice in viewing, at-home purchases, and banking, as well as direct responses to surveys (political views, reading and eating habits, and recreation).

3. There ought to be a fundamental right for every patient to have medical information about himself or herself kept confidential *and* to see his or her own medical information. That is not the case currently.

4. Next, there ought to be a right of every employee to see his or her own personnel record, and a right to be free of intrusive techniques like the polygraph, urinalysis tests, genetic screening, and psychological tests without informed consent. The polygraph ought to be banned in employment especially, because there has been no evidence showing its reliability (Scientific Validity of Polygraph Testing, Office of Technology Assessment, November 1983). The reliability of urinalysis as a means of fairly detecting drug abuse is being seriously challenged; yet many employers are using this technique.

5. There ought to be limits on computer matches that resemble "general searches" that were banned by the drafters of the Fourth Amendment. Without the consent of the individual, the government ought not be able to browse through computerized data banks whose information was gathered in a different context for a different purpose. This does not affect matches of similar data files—state tax files with federal tax files, one state's welfare records with those of a neighboring state, or lists of federal recipients with lists of known dead people.

6. We must find ways to erect barriers between the private and public sectors to prevent the wholesale exchange of personal information without guidelines and precautions.

There is a strong need for a coordinating agency within the Executive Branch to prod the federal agencies, to serve as a clearinghouse, and to accept complaints from the public. The U.S. is alone among the major industrial countries of the West without such a "privacy ombudsman." The Office of Management and Budget has very limited jurisdiction with regard to overseeing the Privacy Act (which covers only federal agencies), and not even all aspects of the Privacy Act. The National Bureau of Standards has some jurisdiction in technical matters. The National Telecommunications and Information Administration in the Department of Commerce, which formerly served this function, has been virtually dismantled.

Most of the nations of Europe have passed data protection laws that limit the export of personal data to the U.S. and elsewhere unless those countries have adequate data protections themselves. This creates a need for U.S. interests to be well represented abroad, by an office that also knows the fine points of privacy law and information policy in the U.S. The office in the Department of State charged with this responsibility is not serving this function.

Most important, the current administration is the first since 1973 not to have an office within the White House to look after privacy issues and develop policy.

CONCLUSION

The right to privacy conflicts with other values in our society—strong law enforcement, efficient government, conservation, and free press. But the privacy side of the equation is usually neglected when government agencies or private organizations build massive data bases or when they decide to ask for more personal information. Privacy is too often an after-thought. And yet there is no evidence that all of this data collection stops crime or reduces fraud. Instead, it places people in a "paper prison." It prompts them to lie or conceal or manipulate—or to resign themselves to cautious, no-risk lives so that credit, insurance, health care, education, or government services are not jeopardized. This negative impact of massive data collection is long-range and gradual. It is rarely part of the equation in high policy circles. There needs to be increased citizen awareness of this negative impact on personal privacy. From that will follow a strong defense in Washington of the citizen's right to privacy.

ATTACHMENTS

- (1) "Privacy Threats Worry Americans," New York Times, 12-8-83 (Harris Poll finds increasing concern);
- (2) "Probing the Capitol's Drug Store," Privacy Journal, 9-83 (release of list of prescription drugs supplied to Members of Congress and Justices of the Supreme Court);
- (3) Ad for computerized pharmacy information;
- (4) "IRS Starts Hunt for Tax Evaders, Using Mail-Order Concerns' Lists," New York Times, 12-25-83;
- (5) "I.R.S. Seeks Links to County Computers in Texas to Find Debtors," New York Times, 3-13-84;
- (6) "The High-Tech Threat to Your Privacy," Changing Times, April 1983;
- (7) "In Defense of Privacy in U.S.," New York Times, 1-21-84 (profile of witness Robert Ellis Smith);
- (8) "Privacy and Videotex Systems," Byte, July 1983 (threats to privacy from home video and computing services).

[From the New York Times, Dec. 8, 1983]

PRIVACY THREATS WORRY AMERICANS

MANY IN SURVEY BELIEVE DATA ON TAXES AND TELEPHONES ARE NOT KEPT SECRET

(By Adam Clymer)

Washington, December 7.—Americans are increasingly concerned about threats to privacy, and about a third of the public believes the Internal Revenue Service, the Federal Bureau of Investigation and telephone companies "probably share" information on individuals with others, according to a poll conducted by Louis Harris and Associates.

Results of the Sept. 1-11 survey of 1,256 people, paid for by Southern New England Telephone Company, were released today as the Smithsonian Institution opened a four-day symposium on "The Road After 1984: High Technology and Human Freedom."

Participants will examine various aspects of society in light of George Orwell's novel "1984," which foresaw an almost all-powerful government.

The telephone poll found the percentage of Americans who said they were "very concerned" about threats to personal privacy increased from 31 percent in 1978 to 48 percent in 1983. It found four Americans in five believed it would be easy for someone to assemble a master file on their lives that would violate their privacy.

SHARING OF INFORMATION

The poll found that 84 percent of the public thought it would be a serious violation of privacy if the revenue service did not keep tax returns confidential, and 82 percent thought it would be serious if the F.B.I. did not keep its data secret.

When asked what they thought actually happened to such data, 36 percent of the respondents said they thought the revenue service shared information and 38 percent said they believed the F.B.I. did. Thirty-three percent said they thought phone companies shared data, although 25 percent said phone companies did not have any information that mattered.

Those agencies were trusted more than several other institutions presented. Fifty percent of the public thought public opinion research concerns shared data, and 51 percent said the Census Bureau, banks and government welfare agencies did so. Fifty-seven percent said they believed insurance companies shared their information, 65 percent said this of loan companies and 75 percent said credit bureaus shared information with others.

Along with the telephone sample of the 1,256 people, the pollsters also interviewed 100 leaders in each of four categories: members of Congress and their aides, corporate executives, science editors and school superintendents. In general, those groups were less fearful of major invasions of privacy than the public was.

LEADERS' OPINIONS DIFFERED

For example, 86 percent in the sample of the public thought it was possible that "a government in Washington will use confidential information to intimidate individuals or groups it feels are its enemies," and 70 percent said that was "likely."

All four leadership groups also said such a development was possible, by about the same percentages as the public. But just 24 percent of the congressional group, 37 percent of the executives, 56 percent of the editors and 39 percent of the school superintendents said it was "likely."

Mr. Harris, chairman and founder of the polling concern, commenting on the findings at a news conference, said he believed "the leadership is far less alerted to the dangers than the people are."

"Those at the throttle of our political leadership just haven't given it much thought," he said.

[From the Privacy Journal, September 1983, vol. IX, No. 11]

PROBING THE CAPITOL'S DRUG STORE

The Freedom of Information and Privacy Acts do not apply to the legislative branch, but some members of Congress may find their privacy diminished because of a court decision involving an anomaly on Capitol Hill.

There is in the Capitol an attending physician to tend to the aches and pains of members and staff. This is a Congressional office, but the physician's office gets its pharmaceutical drugs from the National Naval Medical Center, part of the executive branch. The current Congressional physician is a Navy admiral.

A persistent journalist named Irwin Arieff has requested under the Freedom of Information Act the list of prescription drugs that have been supplied by the Navy to members of Congress and Supreme Court justices over a six-year period. Arieff agreed that the Navy could delete any information that would possibly reveal particular individuals for whom a drug had been prescribed. The Navy refused his request, saying that even from cumulative information it would be possible to figure out what drugs were prescribed for particular individuals or at least for particular ailments.

The Court of Appeals for the District of Columbia, in a unanimous decision this summer, ruled that this "mere possibility" could not prevent the disclosure of the information Arieff is seeking. The court agreed with the journalist that the public has an interest in knowing the quantities of medicine dispensed without charge to Senators, Representatives, and others, as well as whether members are receiving drugs found to be ineffective by the Food and Drug Administration. Judge Antonin Scalia, a former University of Chicago law professor and Assistant Attorney General who is an expert in the Freedom of Information Act, found "justifiable concern" that some members of Congress will be victims of unfair speculation, but said he had no choice but to order the release of information unless there was an actual, not possible, invasion of privacy. *Arieff v. Department of the Navy*, 82-1536 (D.C. Cir. July 22, 1983).

The Department of Justice Civil Division routinely planned to ask the Court of Appeals for a rehearing, but this month asked the court for a 30-day extension in submitting its petition for rehearing "because a number of members of Congress have expressed concern" about the matter. In fact, according to the attorney handling the appeal, the concern came from the counsel for the Senate, a staff member.

Michael Davidson, the counsel, told PRIVACY JOURNAL that there had been no special concern raised since the court decision but that when the litigation began, the Secretary of the Senate and the Clerk of the House, both staffers, stated their concern to the Navy and asked the Navy to protect the interests of Congressional staff and members.

Now for your protection

A Computerized Prescription System at Giant Pharmacies

Giant's new computerized prescription system has many benefits for you and your family.

- Once you provide the information, Giant Pharmacists have your medical and drug history at their fingertips.
- The system warns of harmful effects a prescribed medication will have due to allergies or a medical condition.

- The system warns of harmful combinations of drugs. (Frequently, patients will see more than one doctor and neither doctor may be aware of what the other is prescribing.)

- The system can provide you with a complete record for insurance and tax purposes.

Available at all Washington Area Pharmacies



Barbara Matthews
Lecturer Advisor
to Giant Food

"Please take a moment to fill out a registration form and take advantage of this added safeguard ... at no extra cost to you."

[From the New York Times, Dec. 25, 1983]

IRS STARTS HUNT FOR TAX EVADERS, USING MAIL-ORDER CONCERNS' LISTS

(By David Burnham)

WASHINGTON, December 24.—The Internal Revenue Service has obtained a computerized mail-order list of the estimated incomes of two million American households and has begun to test whether it can help track down people who fail to pay their taxes.

The service is conducting the test despite the refusal of the three major companies that develop such information to provide the Government with a list and over the objections of their trade organization, the Direct Marketing Association.

Alexander Hoffman, who is the chairman of the board of the association and a group vice president at Doubleday & Company, said the sale of the list to the I.R.S. violated a provision in the group's code of ethics that lists should be rented only for marketing and could "upset an important segment of the economy."

The revenue service said a brokerage firm that provides marketing lists, the Dunhill Company of Washington, D.C., had put together the names the agency sought. The association said the company was not one of its members. Officials at the company did not return several telephone calls, but the revenue service spokesman said the names had been put together from several small concerns.

BROOKLYN INCLUDED IN TEST

In the test, a commercially prepared list of two million households in Brooklyn, in Wisconsin, Indiana and Nevada will be matched against an I.R.S. list of people living in these areas who filed income tax returns for the tax year 1982.

All those whose names appear on the first list, but not the second, will be notified that they are subject to a revenue service inquiry about their tax liability. The notices will start going out next spring. An executive of one of the companies objected to the test on the ground that many people who have not done anything wrong would get the notices.

If the test identifies individuals who file no taxes at all, the service will then try to determine whether the same technique can be used to track those who underpay their taxes. According to an I.R.S. plan, the decision whether to use the technique nationwide will not be made until 1985 or later.

A spokesman for the revenue agency said the commercial list it obtained for its test match, after a five-month search, contained the names and addresses of two million households, their estimated incomes, the birthday of the head of each household and the number of people living in each.

In the last few years, the tax agency has become concerned about a slow increase in the number of Americans who fail to pay their taxes. Because of this concern, the agency has sought to develop new techniques for identifying tax evaders.

A recent I.R.S. report on income tax compliance, for example, estimated that revenue losses caused by people compile national mailing lists, the Donnelly Marketing Service of Stamford, Conn., the R.L. Polk Company of Detroit and Metromail of Lincoln, Neb., decided this fall not to sell their information to the tax agency. In separate interviews, officials of the three companies called the project "absolutely ridiculous" and "inappropriate" and indicated it would hurt their business.

The revenue service said in a brokerage firm that provides marketing lists, the Dunhill Company of Washington, D.C., had put together the names the agency sought. Officials at the company did not return several telephone calls, but the revenue service spokesman said the names had been put together from several small concerns.

Mr. Hoffman, the current head of the 2,600-member Direct Marketing Association, said in a telephone interview that he understood that the tax agency had a legitimate concern and that he and his organization hesitated about making "a big public pronouncement" that might affect the Government's ability to handle a real problem.

"But there are some questions we feel the I.R.S. should consider," he said. "What effect will the I.R.S.'s use of mailing lists have on the public's perception about this kind of communication? What I am worried about is that if the I.R.S. is able to undertake this effort on a national basis, it may make the public afraid to have their name on any mailing list, afraid to buy anything by mail, afraid to fill out coupons. By conservative estimates, direct marketing now accounts for sales totaling \$140 billion a year."

DIFFERENCE IS NOTED

Mr. Hoffman said there was a very real difference between the commercial use of a mailing list and the use being explored by the tax agency. "Strangely enough, a mailing list is essentially anonymous," he said. "A company rents a computer tape, prepares one set of labels and makes a mailing. That's it. If you want to have your name removed from a particular list or all lists, our organization operates the Mail Preference Service at East 43d Street in New York where this can be accomplished.

"But if the I.R.S. starts with a commercial mailing list, then adds Census data, then cross references it with other data," Mr. Hoffman continuing, "they then are taking something that is essentially anonymous in the commercial world and turning it into individually identifiable information, using it in a way the individual never imagined."

Noting that the company that was said to have sold the list to the tax agency was not a member of the association, Mr. Hoffman said the sale violated one of the provisions of the group's ethical guidelines, that lists should be rented only "to persons who are going to use them for marketing purposes."

The guideline of the trade organization parallels one of the important principles set out in the Federal Privacy Act. The principle is that information collected by an agency for one purpose should not be used for another purpose without informing the individual who provided the information.

CONCERN AMONG POLLSTERS

The Council of American Survey Research Organizations, representing more than 105 public opinion firms, is also concerned about the tax agency's project.

John Rupp, a lawyer for the council in Washington, said, "We think it would be unethical for the I.R.S. or any other entity to use information obtained from individuals under a promise of confidentiality or to use information in a way that is inconsistent with the purpose for which it initially was collected."

Mr. Rupp added that the council would support the Federal project as long as it was completely based on information in public files. But he added: "In a democracy as complex and varied as ours, that polling plays a pivotal role. We worry that survey or marketing research may not long survive if the trust of the American people is undermined."

Because the original sources of the computerized names provided to the revenue service are unknown, it is not possible to determine how the data were collated.

The method used by the Donnelly Marketing Service, however, involves placing in a computer the names and addresses taken from every telephone book as it is published. The computer is then instructed to assign each household to the correct census tract. From the information published by the Census Bureau, conclusions can be made about each household, including median income, average family size and probable race.

In those states where the information is available on a computerized list, Donnelly then matches data from the Department of Motor Vehicles on the model and year of automobiles owned by the individuals at each address. If the auto is an expensive one, the estimated income is adjusted upward; if it is a cheap model, the income is reduced.

Reginald C. Troncone, the executive vice president of Metromail, recently expressed his concern about the I.R.S. project in a letter to Representative Doug Barnard Jr., the Georgia Democrat who is chairman of the House Government Operations Subcommittee on Commerce, Consumer and Monetary Affairs.

"Our company is caught in the middle," he said. "There isn't any way the I.R.S. can conduct the proposed program and come up with a list of only those individuals who have not filed tax returns. There will be literally millions of legitimate filers who will be contacted by the I.R.S. to provide proof of filing a return."

[From the New York Times, Mar. 13, 1984]

I.R.S. SEEKS LINKS TO COUNTY COMPUTERS IN TEXAS TO FIND DEBTORS

(By David Burnham)

WASHINGTON, March 12.—An Internal Revenue Service office in Texas is seeking to establish electronic links with the computers of 80 counties that will provide it instant access to local records concerning property taxes, voter registration and automobile ownership.

The I.R.S., which already has established such a link with one major county in Texas, said it would use the information to track down individuals who had failed to pay their taxes.

Spokesmen for the revenue agency in Dallas and Washington said the Texas project had not yet been attempted in other sections of the country, and there are no plans for expansion at this time.

The project raises the question of whether the impact of information changes when it can be instantaneously assembled, according to critics of the plan. Although the information that will be transmitted to the service by computer terminals has long been publicly available, the project has generated opposition from conservative Texas politicians and a spokesman for the American Civil Liberties Union.

The criticism voiced by several members of the commission that governs Tarrant County, the area around Fort Worth, was so sharp that two weeks ago the I.R.S. withdrew its proposal to establish a direct link with that county's computers.

OFFICIAL FEAR EFFECTS

"This was just another extension of the drive by the Federal Government to gradually increase its power over local government," said B.D. Griffin, a Tarrant County commissioner.

Secretary of State John Fainter raised another objection, saying, "The specter of the I.R.S. having direct access to voter registration records may intimidate those persons considering registering to vote."

But Glenn Cagle, the director of the revenue service district that covers 143 counties of northern Texas, defended his plan as a way of reducing the costs of gaining information the Government could obtain anyway and said he was surprised by the opposition.

"I am not going to speculate on the motives of the critics," he said, "But the fact is this is an election year."

An I.R.S. spokesman in Washington, Scott Waffle, said he too was surprised by the adverse reaction. "All that is happening down there is an effort to improve the Government's efficiency by lessening the cost of obtaining information that always has been available to anyone who asks for it," he said.

Mr. Waffle added that the project was not the result of a national directive to the I.R.S.'s 63 districts and that as far as he knew was not currently being pursued in other regions.

The district that is moving to develop direct computer links has its headquarters in Dallas. In 1982, the individuals and businesses within its borders filed 4,858,821 of the 171 million tax returns the agency received.

Last summer, Mr. Cagle wrote each of the counties requesting information about the extent to which their records were computerized and whether they would be interested in the project to give the I.R.S. direct access to them.

Marlene Gaysek, an agency public affairs official in Dallas, said the district was negotiating with 80 of the counties and expects to complete arrangements with 20 of them soon.

According to the contract that has been signed with Dallas County, which has 1,644,000 residents, the revenue service will have a county terminal in its Dallas office that will allow its 2,000 employees to make nearly instantaneous checks about the property owned and the property taxes paid by every person in the county; the name and address of all persons with a registered vehicle; the make, year and weight of that vehicle, and the name and address of every registered voter.

Although the I.R.S. requested access to all the data in the voter registration files, the Dallas County commissioners rule the agency could not obtain the dates of birth, Social Security numbers or telephone numbers of individuals.

Miss Gaysek said the computer links would save the agency about \$200,000 a year because lower-paid clerks, rather than field agents, would be able to gather information, and travel costs would be avoided.

She said the district office would not use its computer access to compile complete new lists of all individuals living in an area that then would be matched against computerized lists of taxpayers.

"There has been a real misunderstanding," she said. "We're not taking wholesale lists for computer matching purposes, we are using our direct access to track individual taxpayers. We need this detailed information when we file a tax lien against someone or check to make sure a taxpayer's financial statement is correct."

PRIVACY ISSUE RAISED

James C. Harrington, an attorney in the state office of the A.C.L.U. in Austin, said that even though the information the I.R.S. would receive by computer was public, the use of county data conflicted with one of Congress' chief goals in protecting Federal records: a guarantee in the Privacy Act that the information an individual provides the Government for one purpose will not be used for another without the individual's permission.

"We generally oppose this kind of cross computerization because despite what any agency says, history tells us that the information the I.R.S. is collecting will be compiled into a giant centralized data base," he said. "History also teaches that we have to develop appropriate legal restraints on all Government agencies."

Tony Bonilla, the chairman of the National Hispanic Leadership Conference, said: "The bottom line is that this project is not necessary. The I.R.S. already has enough information about every taxpayer."

[From the Changing Times, April 1983]

THE HIGH-TECH THREAT TO YOUR PRIVACY

If you think computers know a lot about you now, just wait. Prospects for the years ahead make the need for privacy safeguards increasingly urgent.

Welcome to the world of the American consumer, circa 1990:

That deck of credit cards you used to carry around in your wallet is a nuisance of the past, replaced by a single "smart" card. In its computerchip memory resides easily retrievable data about your bank balance, your credit rating, even the status of your health insurance. Thus equipped, you have instant access to all manner of goods and services with little or no hassle.

Thanks to computer-assisted hookups with local stores and banks, your television set now serves as an inhome buying and banking tool. If you want to use it the old-fashioned way, your choice of what to watch at any given time is almost endless because a central computerized "library" lets you call up any of hundreds of programs ranging from religious services to adult movies. And, if you're so inclined, you can take advantage of frequent opportunities to register your opinions on political and social issues by pushing the prescribed buttons in response to questions on the screen.

Computerized correspondence has largely done away with paper-and-pencil letter writing. Instead, you use an electronic mail system to flash your messages practically anywhere in the world in an instant. You get your answer via your home computer or TV screen.

Futuristic? Hardly. The technology that makes all this possible already exists; it seems only a matter of time before such scenes are common.

It's a prospect that has a lot of people worried. In all likelihood the data on a smart card will be recorded and stored in a computer file so that a verification will be available for legal purposes. Each time you use your TV set to make a purchase or choose a program or register an opinion, a record will be made of it. Each time you send or receive an electronic letter, a record will be made of where it went and where it came from.

Records such as these can reveal a lot about your private affairs that you probably wouldn't want very many people to know. This is why many privacy experts, contemplating the potential misuse of the wealth of information being compiled on individuals, consider computers a more serious threat to privacy than any other technological development of the 20th century. However, they stress that if proper safeguards are included, protection and confidentiality are possible with computers.

The question boils down to this: What guarantees do private citizens have that these records won't be used against them by the businesses or government agencies that have access to them?

THE THREATS TO PRIVACY

There are some federal and state laws already on the books to protect privacy, and some two-way television and computer companies have developed privacy codes of their own. But the collection and computerizing of personal information about you is proceeding at such a rapid rate that technological developments are rendering past protections obsolete.

Arthur Bushkin, who worked on privacy issues in the Carter administration and is now a Washington consultant, sees three major threats.

Eavesdropping.—Wiretapping and interception of private radio communications is generally prohibited by federal and state laws. Law enforcement agents, for example, usually cannot engage in wiretapping without a court order. But eavesdropping on radio communications has become easier with the development of sophisticated scanners.

Privacy of records.—This is Bushkin's principal area of concern. "The catalyst here is the computer and its magnificent ability to store and disseminate information," he says. Businesses, banks, governments and other institutions have been putting together fairly extensive records on all of us for a long time, but once records are fed into computers, it is possible not only to compile more information faster but also to provide almost instant access to it by people unknown to us and for reasons never stated to us.

Surveillance.—"Computers," notes Bushkin, "can follow you around." We may soon be leaving a computerized trail not only of our financial transactions but also of our movements and habits. Credit-card transactions already leave a trail, and the smart card may reveal even more about you.

"We may soon be leaving a computerized trail not only of financial transactions but also of our movements and habits."

"During the next two decades," Bushkin predicts, "we will become a wired nation. We will have the inherent capability to build up a much broader profile of people's habits and track the location of behavior. This will force us to examine some very fundamental questions about the kind of society we are."

Computer systems offer great potential for law enforcement, Bushkin believes. It will probably be possible to program them to find someone who is on the FBI's ten-most-wanted list. "On the other hand," he asks, "do we want to use these systems to search for people with more than three outstanding parking tickets?"

Robert Ellis Smith, publisher of *Privacy Journal*, a monthly newsletter, fears that two-way television will create the major privacy problems of the future. Two-way television is a form of pay TV, he notes. The companies providing the programs and services must know when and how the systems are being used so that they can bill their customers. The byproduct of the billings is a computerized record of household habits.

Two-way TV can also provide burglar and fire alarm services. But to activate some systems, you must tell the company providing the services that you are leaving your home, thus creating a record of your comings and goings.

Smith, author of *Privacy: How to Protect What's Left of It* (Doubleday), is also concerned about the ability of two-way TV and smart cards to monitor consumers' behavior without their knowledge.

He cites a recent experiment in Pittsfield, Mass., where consumers—voluntarily, in this case—agreed to have their purchases recorded to see how they were responding to television advertising. The bar codes found on virtually all packaged goods make it easy to track purchases. In the Pittsfield experiment, purchases were measured through the use of consumer identity cards as well as the bar codes. Such experiments, Smith fears, could be duplicated by examining the records of smart card and TV purchases without consumers' knowledge.

SIZING UP THE SAFEGUARDS

Warner Amex Cable Communications, which operates the two-way interactive cable television service QUBE in cities in Ohio and several other states, is sensitive to the privacy issue. The company's 11-point Code of Privacy states that Warner Amex "shall maintain adequate safeguards to ensure the physical security and confidentiality of any subscriber information." The code also provides that information about individual subscriber viewing or responses "will be kept strictly confidential unless publication is an inherent part of the service (e.g., announcing a game show prizewinner)" and that Warner Amex "will refuse requests to make any individual subscriber information available to government agencies in the absence of legal compulsion. . . . If requests for such information are made, Warner Amex will promptly notify the subscriber prior to responding if permitted to do so by law."

Warner Amex's code has been tested at least once, and the company has stuck by its pledge. When a movie theater operator in Columbus, Ohio, was accused of showing a pornographic film, he protested that the film had already been on the QUBE cable system in Columbus and asked the company for the names of the people who watched it. A judge ruled that Warner Amex need not provide individual names, but the company was ordered to make public the percentage of its subscribers that ordered the movie and presumably saw it as well.

On a broader scale, only three states—California, Illinois and Wisconsin—now have laws seeking to insure privacy for subscribers to cable systems and two-way TV. The provisions are similar to the Warner Amex code. In addition, the California law prohibits a cable system operator from using “any electronic device to record, transmit, or observe any events or listen to, record, or monitor any conversations which take place inside a subscriber’s residence, workplace, or place of business, without obtaining the express written consent of the subscriber.”

This section, which is similar to one in the Illinois law, is designed to protect people from abuse of systems that, in effect, listen in to homes in order to provide fire and security protection. One such system links a TV set to a computer monitor capable of electronically sweeping a household every seven seconds.

So far, the interest in privacy-protection laws on a national scale is practically nil in Washington. A report on privacy dangers was issued by a special presidential commission six years ago. Its recommendations have not been enacted by federal agencies or Congress. Congressional hearings will be held this spring on safeguards for the use of tax information.

Little more than a decade ago, in fact, proposals were made for a centralized federal computer list that would combine all the information the government had about an individual, from social security records to military service and even arrest records. The proposals, which were backed and pushed largely by law-enforcement agencies, never got serious consideration.

Today there is no longer any talk about centralizing information because computer techniques have advanced so quickly that one master file is unnecessary. The same purpose can be served by computer matching programs. Two or more tapes containing different kinds of information can be run through a computer and compared to discover which names or information appear on both lists.

Such matching of tapes is being performed to find people suspected of being welfare cheats and government workers who have failed to pay their federal student loans, and to identify youths who have not registered with the Selective Service System. In the last case, the social security numbers of youths who reach registration age are checked against selective service and armed forces lists. If a name on the social security list is not on the selective service or armed forces lists, the government scores a “hit” and provides the Selective Service System with the name and address of that person.

WHAT’S LEGAL?

Information gathered about all of us by the government is supposed to be used only for the purpose for which it is obtained. But the interpretation of laws and regulations differs, and new laws can be passed. The Privacy Act of 1974, which spells out the rules for government agencies, restricts the use and disclosure of information. However, the selective service matching program was specifically authorized by Congress, and federal guidelines have been revised to facilitate computer checking for welfare cheats and delinquent student loans and to leave more discretion to individual federal agencies.

Henry Geller, former head of the National Telecommunications and Information Administration, a federal agency within the Department of Commerce, contends that for sensitive information there must be “an expectation of confidentiality” of information obtained from individuals by the government or anyone else. The U.S. Postal Service and the Internal Revenue Service have generally good records of protecting the privacy of the mails and sensitive tax information, says Geller, who is now a Duke University professor.

People worried about computer-assisted invasions of privacy insist that they do not want to thwart the computer industry. Rather, they say they seek a balance between technological advancement and citizens’ well-established right of privacy.

“What makes America unique,” says Geller, “is its treatment of the individual, and that must include a guarantee of the right of privacy. It is a part of the quality of life. Privacy and the dignity of the individual go together.”

[From the New York Times, Jan. 21, 1984]

IN DEFENSE OF PUBLIC PRIVACY IN U.S.

(By David Burnham)

WASHINGTON, January 20.—From a one-room office on the second floor of the carriage house behind his Capitol Hill home, Robert Ellis Smith, a 43-year-old lawyer

and former newspaper reporter, sounds the alarm about maintaining freedom and privacy in the computer age.

Now entering his 10th year as the owner, publisher and principal reporter of *Privacy Journal*, a monthly newsletter that charts the impact of technology on the rights of the American people, Mr. Smith, a kind of one-man lobby, worries that today, as much as ever, the nation is threatened by the widespread intrusions described in "Nineteen Eighty-Four," George Orwell's novel.

"We haven't reached the Orwellian nightmare yet, in part because the Government is somewhat inefficient," he said recently. "But what we are allowing the computers to do to our society is still quite upsetting. We seem to feel that the computers have so much information about us that we shouldn't take any risks, that we should be compliant people."

Mr. Smith says public interest in privacy issues reached a peak in the period 1975 to 1977, when abuses of Government power were uncovered in the Congressional investigations of the Watergate scandals and activities of the Central Intelligence Agency, resulting in the creation of the Privacy Protection Study Commission, which issued a national report in 1977. "But with 1984 here," he added, "issues raised in George Orwell's novel seem to have revived a good deal of interest about where our society really is headed."

REGULATIONS ABOUT PRIVACY

Because the great Federal agencies such as the Internal Revenue Service, the Federal Bureau of Investigation and the National Security Agency have headquarters here, Washington is the fountain of regulations affecting individual privacy and thus the natural base for Mr. Smith.

Congress frequently holds hearings about privacy abuses concerning both the Government and private industry and periodically passes legislation dealing with privacy, such as the Privacy Act, a law that gives Americans certain information rights, including the power to see and correct records held about them by Federal agencies.

The Congressional Record, court decisions and obscure regulations published in the Federal Register are the raw materials of Mr. Smith's newsletter. Occasionally a Congressional hearing will lure him out of his office. Often he gets tips from officials who share his concerns.

"Since my first days as a reporter, the struggle of the individual against the institution always has been one of my central interests," Mr. Smith said of his work. On one wall of his spacious, sunny office, situated just seven blocks from the Capitol, book shelves bulge with reports and studies and other volumes touching on the hundreds of different issues that concern him. A small cast-iron stove and a stack of wood take up a good portion of another wall.

PERNICIOUS TECHNOLOGY

One bit of noncomputer technology that Mr. Smith had devoted many articles to in his neatly printed newsletter is the polygraph, or lie detector, a device designed to measure the stress felt by a subject when he is asked a series of questions. The polygraph is now routinely used within the C.I.A. and the National Security Agency to try to anticipate security problems.

Last year the Reagan Administration issued a directive vastly expanding the use of the polygraph for investigating the unauthorized disclosures of sensitive information, but Congress recently approved legislation postponing these procedures until this spring.

"Government and business use this pernicious technology in a way to convince people that machines can do something that people cannot, that machines can get into someone's brain," Mr. Smith said, "I agree with those who describe polygraphs as 20th-century witchcraft, a modern version of the Medieval world's trial by fire."

Mr. Smith is critical of how Government has responded to the challenge of the new technology. "The Supreme Court under Chief Justice Warren Burger has taken a restrictive view about privacy rights," he observed. "If the invasion did not occur in the marital bedroom, the Court seems to feel there has been no invasion at all. Also, most of the Federal courts have been slow to recognize that the new computer technologies can elevate an action which once was not important to an action that poses significant constitutional question."

Mr. Smith believes, however, that one of the fundamental problems may lie in the Constitution itself. "The Constitution imposes no restriction on the actions of private corporation, only on Government agencies," he said. "The Founding Fathers established a system of checks and balances for the Government. For most people, being searched by the police is a remote possibility. But being subjected to physical

searches by your employer or computer searches by insurance companies and credit reporting companies is quite likely.

Mr. Smith charges \$89 a year for his newsletter, which now has a monthly circulation of about 1,500 down from a peak of 2,000 in the post Watergate years in the mid-1970's. He said there had been a recent surge in sales.

"I don't see any signs that the trend toward more and more control of the individual is being retarded," he said, "but I'm not going to stop trying."

[From the BYTE Publication, Inc., July 1983]

PRIVACY AND VIDEOTEX SYSTEMS

TWO-WAY SERVICES BRING WITH THEM THE POTENTIAL FOR ABUSE

(By Richard M. Neustadt and M. Anne Swanson)

Midway through George Orwell's 1984, the hero meets an old man and asks him how "Big Brother" got started. Things began to go wrong, the old man answered, when someone invented two-way television.

Advances in telecommunications promise to bring all sorts of conveniences to our doorsteps. We'll be shopping, banking, and working from home. We'll have computer-controlled electronic mail, burglar and fire alarms, and medical alerts, among other things. But along with this array of new services and products comes a potential for abuse.

The possible threat to privacy that home video and computing services pose is beginning to worry some people. The growth of nationwide videotex systems, whether they operate over cable TV or telephone lines, presents two major causes for concern. First companies that sell electronic information or provide transactional services such as home banking and shopping will be able to compile dossiers on their subscribers. This information could be misused. Second, the proliferation of electronic transfer of information raises new questions about wiretapping.

DATA COLLECTION AND DISCLOSURE

The current debate focuses on the collection and possible misuse of subscriber records. Most companies that provide videotex services generate files on subscriber behavior as a matter of course. For instance, if the system operator provides information and charges his customers on a per-page basis, then his computer must keep a record of every video page subscribers request. If the system is used for transactions such as shopping or banking at home, the retailer or financial institution must keep a record, and the cable or telephone system operator may want to keep its own record as protection against claims of error.

Most companies that provide videotex services generate files on subscriber behavior as a matter of course.

Of course, similar records have always been collected by banks, hospitals, insurance companies, and other institutions. But with videotex systems, more records are being collected in one place. Moreover, computer files are easier to obtain than original documents.

The concern about collection of records leads to another issue: the possible disclosure of private information on consumer behavior. System operators may want to sell this data to retailers, pollsters, direct mailers, or credit investigators. Such information is commercially valuable, as indicated by the similar active market in magazine subscription lists.

The action of a theater owner in Columbus, Ohio—where Warner-Annex runs its interactive Qube service—is an example of data disclosure. The owner of the theater subpoenaed lists of people who had watched "adult" movies on cable TV in order to defend himself against obscenity charges for screening those movies in his theater.

PROTECTING PRIVACY

Without a law or service contract to the contrary, company records belongs to the company that collects them, not to the subscriber. The United States Supreme Court established this principle in 1976 when it held that a consumer had no constitutionally protected interest in his bank records that would enable him to challenge their release to government officials.

In the last two years, however, a movement has taken wing to legislate protections for those records. California, Illinois, and Wisconsin have passed privacy laws,

six other states are seriously considering such measures, and the U.S. Congress may well pass a privacy law next year. While most of these bills are aimed at cable TV, the Illinois law and several of the proposed bills also cover two-way services provided over telephone lines. In addition, most cable TV franchises issued in recent years include privacy rules.

The central aim of this legislation is to require the system operator to obtain the subscriber's consent before collecting information. In most cases, collection without consent is allowed only for purposes of billing, providing a service like at-home shopping, or protecting against unauthorized reception or other services.

The measures vary on specifics. The Wisconsin law goes so far as to require cable operators to offer subscribers a free on-off switch controlling the interactive service. Some of the pending bills require system operators to acquire liability insurance to cover any suits based on violation of their privacy provisions.

Many people in the videotex field feel that all this legislation is unnecessary. They argue that there has been no evidence of abuse and that system operators are hardly likely to offend their customers by invading their privacy. These companies make a strong argument that we should wait to set rules until we know more about the market and the technology.

Legislation is beginning to look inevitable, however. And when it does pass, the biggest problem for the videotex industry will be the motley of state and local rules and the often ambiguous wording of laws. The differences from law to law would, for example, require the operator of a system serving several states to maintain separate data bases and procedures for each state—a costly proposition.

Some companies providing interactive services see self-regulation as the best way to allay subscriber concerns and avoid a patchwork of conflicting rules. Two large cable firms—Warner-Amex and Cox—have issued codes of behavior regarding privacy. The National Cable Television Association and the Videotex Industry Association have formed groups to draft industry-wide guidelines. Meanwhile, there is increasing support for a uniform standard, set by Congress, to preempt state and local rules.

INTERCEPTION

In the case of interactive systems, several kinds of interception are possible. An eavesdropper—or a law-enforcement agent—would put a physical tap on a telephone line or dial into a central computer that transmits messages and keeps records. A cable subscriber could use special equipment to listen on his cable and pick up signals addressed to or transmitted by other subscribers.

Federal law provides criminal sanctions against unauthorized interception of wire communications and regulates legal wiretapping by law-enforcement authorities. The law allows government agencies to wiretap, but only with a court order—which the courts are to grant sparingly—or, if national security is at issue, pursuant to an order from the Attorney General.

Unfortunately, the drafters of this law—who worked on it almost 15 years ago—did not anticipate advances in technology, and the law now has two large loopholes. First, the law covers only "aural interception," so it does not seem to apply to eavesdropping on data and text transmissions, such as electronic mail. Second, the law defines "wire communications" as transmission provided by common carriers such as the telephone company—probably omitting most cable services.

Legislation pending in Congress addresses both problems. Senate Bill 66 forbids any private person or government body from intercepting any broadband communication unless authorized to do so by the system operator, program originator, or federal law. (The provision does not specify whether law-enforcement investigators would use a regular search warrant or would have to meet the wiretapping law's strict standard to get court permission for nonaural interception.) This same proposal defines cable transmission as "wire communications" so as to include them within the law's scope.

It is too early to tell whether the privacy legislation pending in Congress will become law. If it does, it would preempt similar state regulation and would provide a unified substitute for the hodgepodge of different state and local rules. Although the federal proposal is currently part of a bill that focuses on cable systems, it is drafted broadly enough so that its provisions could be interpreted to include telephone-based services as well.

In the meantime, industry attempts at self-regulation on the privacy issue will increase. Most system operators are anxious not to scare their subscribers—it's hard enough to sell a new product without introducing fear into the equation. As a result, the Orwellian scenario may remain more fiction than fact.

Mr. KASTENMEIER. Thank you very much, Mr. Smith, for that very interesting account.

I understand that the interaction among these many entities, mostly in the private sector but some in the public sector, in terms of access to information in other entity systems, is done on some sort of an exchange basis. The exchange is negotiated between one agency, whether it is a credit bureau and a Federal agency, or any others on a voluntary basis. That is to say, one, there is not normally access provided pursuant to law or; two, it is not, for the most part, involuntary. One system does not have access to another system without the second system's knowing about it or having made arrangements to grant the first system computer access; is that not the case?

I ask that because I am not clear in terms of computer technology what the relationship is of computers and data bases in different entities, and how it is that these various entities make arrangements for exchange of information, or access to information.

Mr. SMITH. Your understanding is correct. I don't know of any automated exchange of information that is mandated by legal process by subpoena or anything of that sort. There is legal process, of course, when a FBI investigator would go to a bank; but that is for just an individual access to information. But on an automated basis—these are all voluntary, the Federal agencies pay for that information.

You will have testimony later in the morning that mailing list companies don't want to cooperate with the Internal Revenue Service and they are not obligated to, there is no legal obligation to participate; so it is negotiated.

The Federal agencies right now are putting out requests for proposals for contractual arrangements between themselves and the credit bureaus.

Mr. KASTENMEIER. Should the Congress evolve a policy, or develop an attitude about such voluntary exchanges? Precisely what is it that we can do about this if we feel it is pernicious?

Mr. SMITH. I think some sort of barrier should be erected between private and public because different standards apply, different constitutional protections apply. I have not gotten to the point where I can actually devise the guidelines that you would come up with. But the first question when the Internal Revenue Service wanted access to mailing lists was: Is it illegal? And it is not illegal. I think that we should anticipate that there is going to be more of this and the Congress ought to, I guess, draw the line. I can't be more specific than that. But I think it is something that we have to look into.

Mr. KASTENMEIER. We are told that the computer field is going in a direction where a computer terminal that you have in your office or even in your home, might have potential access to all sorts of other systems. The result is that the information may be more freely accessible. Therefore, we do have to ask ourselves, in the public interest, what information is being exchanged and how does it impact on the unknowing and the innocent.

Mr. SMITH. I agree. We can't forget that the computer hackers in Milwaukee got into the Sloan-Kettering Cancer Center, which has very sensitive patient information; that most of the computer

crimes involve banks. From my participation in trade conferences, I find them very vulnerable. In fact, most security directors of banks and of hospitals and like organizations, really, are relying on blind luck. I don't think they have any precautions to prevent access to these systems.

I am not enough of a technologist to know whether if you get access to part of this network, you can proceed on to other aspects of it; I think not at this point. But we do know that many of the entities on this chart have been compromised.

Mr. KASTENMEIER. I note that one of your newsletter articles of last September dealt with the probing of the Capitol's drugstore in which an individual sought, under the Freedom of Information Act, access to a list of prescription drugs that had been supplied to Members of Congress and Supreme Court Justices over a 6-year period.

Mr. GLICKMAN. You mean it has gotten that far, Mr. Chairman?

Mr. KASTENMEIER. There is apparently a pending court case. I don't know if there is anything further on that. But that should suggest, at least for comparison purposes, what the potential is for anyone to obtain access to medical information. Medical information may or may not be protected.

Mr. SMITH. The Freedom of Information Act, of course, doesn't cover the Congress, but there is that one component of the executive branch, apparently, that administers some of the pharmaceuticals here on the Hill (The Office of the Attending Physician).

Mr. KASTENMEIER. Yes.

Mr. SMITH. It was an anomaly of the law.

Mr. KASTENMEIER. On another subject, is the Fair Credit Reporting Act working, do you think?

Mr. SMITH. I think fairly well. It does not require that the credit bureau give you an actual copy of your record, only that you be told what is in it. Most credit bureaus have a policy of giving you a copy, so in practice I guess it is working OK; but I think that is a loophole in the act.

One other problem that I think should be addressed is that when you do see information in the credit bureau you are banned by the law from suing for an invasion of privacy, for slander, based on the information that you find. I think that immunity is improper.

Mr. KASTENMEIER. I think those of us who have served in Congress a while felt that we made some giant steps forward in the late sixties and early seventies, not just in the Privacy Act but with reference to practices that had been conducted between the Government and other entities affecting individuals.

For example, it used to be rather common for banks and for the telephone company to permit agents of the Federal Government access to information either through wiretapping or through access to accounts. After a number of disclosures of such access, those institutions decided that, for their own protection, they were no longer going to accommodate sub rosa the requests of Federal agents to intrude in the affairs of others. Therefore, Congress provided that one would have to obtain a warrant, for a search of accounts or wiretapping.

But with the development of the computer, it seems that there is a departure from that requirement just because of the technology itself.

I would like to yield to my colleague from Kansas who serves on the Science and Technology Committee and is also very interested in this question. I yield to Mr. Glickman.

Mr. GLICKMAN. Thank you, Mr. Chairman.

First of all, I want to thank you for an excellent statement. I chair a Subcommittee on Communications in the Science Committee. Largely with the help of Louise Becker at the Library of Congress, we put together 3 days of hearings; we had Neil Patrick from Milwaukee testify. In fact, we are going to issue a committee report next week.

One of the things that we found is that the subject is so complicated that you just can't deal with it in small segments, like privacy, like technology changes, like Government role. They are all so interrelated that the tendency here in Congress is to want to enact a statute that would make computer trespassing a crime, when in fact that is just a tiny segment of the problem. Privacy is an even bigger part of the problem than mere trespassing. How does the whole thing relate, for example, to the interrelationship between Government communication systems? You point out with some of your pictures and graphs, the interrelationships between the electric utility system, the air traffic control system, and the banking system.

I guess I would ask you this question: I think a lot of things that you say are just right on target. It looks to me like the subject matter is so overwhelming that unless we have some sort of institutional mechanism to look at it in a more comprehensive way we will continue to kind of pick apart at it and pass this one little computer trespass bill, which really doesn't do very much.

I wonder if you might comment on that.

Mr. SMITH. I absolutely agree. I think these hearings are unique, because you have not been reluctant to go outside jurisdictional boundaries, and I think that is so important. You just can't confine it to one category, absolutely, because it goes into both sectors and all aspects of our society, and it is a technological as well as a legal problem.

One thing is to develop principles that would apply to all data collection. I think that is important. You do stumble into problems there as well, because a certain principle that might make sense with regard to medical information, doesn't make sense with regard to welfare information.

I endorse your view, that you have to take a much larger view of the whole thing. I think that safeguards with regard to misuse of computers is an important component of that and I think that prohibiting the criminal misuse of computer systems certainly goes a long way in protecting these records. So that passed by itself, a computer crime law would not do any harm, certainly it is part of the issue.

Mr. GLICKMAN. How would you feel about some sort of a national commission on privacy in communications? Willis Ware and others have testified. The feeling is that elevating the problem to a question of greater national attention in trying to pull it out of the spe-

cific smaller parochial interests can't be done unless you set up some sort of a national think tank or something along those lines.

Mr. SMITH. We had a commission in the last decade and that did help somewhat, but it also broke down the issue into its minutia as well. It came up with some 65 recommendations and missed a large part of the grander picture.

I guess I am reluctant to say let's go the commission route again. Something along that order, though, I think is really needed.

Mr. GLICKMAN. I would like you to amplify your statement on page 8 of your written testimony: OMB agreements with Federal agencies will be permitted to have access to individual credit reports stored by seven different companies.

Which Federal agencies are we talking about? What kind of information are we going to give these Federal agencies?

Mr. SMITH. It was authorized by Congress in the Debt Collection Act of 1982. But when you see it in the actual black-and-white type of a request for proposals it is rather shocking to see.

These would be any agencies that have a loan relationship with an individual: Small Business Administration, the Department of Education, the Veterans' Administration, HUD, those types of agencies. OMB is sort of coordinating all of this.

They would simply allow for a computer terminal in the office of anybody who is in charge of processing Government loans.

Mr. GLICKMAN. So you could go right out and pick up all the information the XYZ Credit Corp. has, let's say on me—

Mr. SMITH. Yes.

Mr. GLICKMAN [continuing]. And that would go into HUD's housing collection department, or student loan collection department at the Department of Education. And they could see a whole assortment of information, whatever is stored in that credit file, that perhaps may be totally unrelated to the collection of that debt.

Mr. SMITH. It might be related. It would tell what bank you deal with, and whether you have any loans there, any outstanding balance of the loan. It would list all of the department stores and the major oil companies you do business with. And then a code from zero to nine indicating how successful that account is.

Then also, as I indicate, there is some narrative information that comes from the courthouse—liens, arrest records.

Mr. GLICKMAN. Has OMB provided any guidance yet to these agencies on how to use or not use this information, or what kind of guidelines there are?

Mr. SMITH. That always comes after the fact, unfortunately.

Mr. GLICKMAN. So there is nothing so far, then?

Mr. SMITH. No; there isn't. The Fair Credit Reporting Act will prohibit, for instance, the Department of Education or any other agency from using that computer terminal for anything but loan purposes. But how you enforce that, I don't know. Why somebody can't come in on a Saturday morning and use that terminal to check out his future brother-in-law, I don't know; there is no prohibition.

Mr. GLICKMAN. Expand upon this thing about life styles. Is the IRS now renting computerized lists that provide demographic profiles of various households so they can find out if I go to the

movies, or the Lion D'or for dinner, or Las Vegas for a weekend, and then determine if I am not paying enough in taxes?

Mr. SMITH. Well, not quite that data, but they could indicate that you had a Cadillac and a Ford.

Mr. GLICKMAN. But could they look into, let's say, my American Express account?

Mr. SMITH. Not into it; the fact that you had such an account might be reflected, and the general balance that you keep, that might be in there, yes.

Mr. GLICKMAN. Well, the general balance I keep might give some idea of what kind of charges I have.

Mr. SMITH. That is right, but not the specifics of your account, that would not be reflected on these lists.

Mr. GLICKMAN. Are there any limits on how the IRS can use those lists?

Mr. SMITH. None at all. We ought to refer to that chart, No. 3, that tells the whole list of information that is available, it includes ethnic groups and religion as well. I just think every other Federal agency is going to want access to that. But it does not include the specifics of an account or the charges of your account.

Mr. GLICKMAN. What about the technology of protection of computer information? I mean, in the same way that the computer technology has advanced so dramatically, has defensive technology advanced as well? Has the use of control mechanisms, innovative ways of scrambling, passwords, all those kinds of things moved as fast as the basic technology in the last 10 or 15 years?

Mr. SMITH. I believe it has, perhaps even faster. I am not sure it has been employed to the same extent. I think a lot of companies don't make the investment, they are really relying on luck. But the technology in computer security is the least of our problems because that is moving apace.

Mr. GLICKMAN. How involved is the insurance industry in encouraging their clients in the private sector to protect the integrity of the information that is stored in the computers and the computers themselves? That is, I would think if the insurance industry would fail to provide liability insurance for people who didn't adequately protect their computers, it might encourage a lot more protection for the average citizen in the process.

Mr. SMITH. Exactly. You see that with regard to home and fire protection, and health protection, and auto coverage. But I haven't seen any evidence yet that the insurers are taking a lead in this. Maybe they are but I haven't seen it.

We are at the stage right now where if computer crime is discovered in a company, it is suppressed, and the individual is either let go or given a promotion; you know, anything to keep it quiet. That is where we are now.

Mr. GLICKMAN. Thank you, Mr. Chairman.

Mr. KASTENMEIER. The gentleman from California, Mr. Berman?

Mr. BERMAN. No questions.

Mr. KASTENMEIER. Mr. Smith, we would like to thank you for your appearance and your help this morning. Your testimony is very useful and we are pleased to avail ourselves of your views on these matters.

Mr. SMITH. Thank you.

Mr. KASTENMEIER. The Chair would like to call as our next witness, Prof. Kenneth C. Laudon, professor of computer applications at the New York University of Graduate School of Business.

Professor Laudon is the author of several books directly relevant to today's hearing: "Computers and Bureaucratic Reform," "Communications Technology and Democratic Participation," and the forthcoming "Security, Freedom and Efficiency. Value Choices in the Design of National Information Systems."

Professor Laudon, I welcome you this morning and you may proceed as you wish.

TESTIMONY OF KENNETH C. LAUDON, PROFESSOR OF COMPUTER APPLICATIONS, NEW YORK UNIVERSITY GRADUATE SCHOOL OF BUSINESS

Mr. LAUDON. Thank you very much. The forces of chaos and disorder have made it very difficult to appear before you. I am happy to see that you do have a copy of my statement. And I am happy to say I was able to find my way out of LaGuardia Airport in the fog this morning, and it is a pleasure to be here.

I have worked in the information systems area since the late 1960's when I began a series of studies on how third generation computers affect public decisionmaking. I have worked at the Federal level as a consultant to the Office of Technology Assessment and their studies of a number of national information systems such as the Internal Revenue Service, Tax Administration System, in 1977. I was a member of a research team for System Development Corp.'s review of a proposed Social Security system in 1978.

In 1979, I began a 3-year effort as a contractor to the Office of Technology Assessment study of the National Crime Information Center proposed by the FBI.

In my view, society as a whole and Members of Congress in particular, have some difficult decisions to make about which values will reign supreme in the design of systems.

I see these values as choices among international and domestic security, efficiency or civil liberties.

In my experience with specific national information systems over the last 5 years, I have found many aspects of proposed systems that are threatening to civil liberties.

Bob Smith has already pointed out to you a number of trends in the development of systems with his excellent charts and illustrations. It seems to me, Bob Smith pointed to three things. One is the increasing density of linkages between Government computer systems and Government and private sector systems.

This chart that Bob has reproduced here on page 13 is just an excellent illustration of the kinds of linkages that exist now; within a decade you should expect this chart to look like a solid black line.

Ten years ago, it might have been said that there would be an increasing density of linkages between systems. Ten years ago was just when data-base management technology was coming on line. People predicted then that these kinds of charts would be commonplace by the 1980's. We can predict confidently today that by 1990, this chart will be a solid black line. These linkages won't be infor-

mal linkages, they will be formalized linkages that are made possible by advances in data base management and technology.

In addition, Bob pointed to two other trends I would just like to highlight here. First, there are new uses for information being found. New data bases are being created; the purchase by the IRS of private sector credit data information is the creation of a new data base by the government. There is just no other way you can label that.

Second of all, new uses are being found for information. In these situations, we have an existing data base which becomes automated and more accessible, and new uses follow from that. New organizations are attracted to data bases like bees to honey.

A third trend that Bob pointed to is the idea—we could have stated this 5 years ago—of the executive branch flexing its data processing muscles and circumventing privacy controls, which Congress originated in the 1970's to constrain executive branch uses of information.

I am going to point to those in my testimony and underscore some of these trends and add a few of my own.

Based on my specific experiences with systems such as the FBI system and Internal Revenue and Social Security over the last 5 years, one of the major threats to civil liberties that I see is this major extension in data surveillance capability for minuscule gains in security and efficiency.

It is unclear to me, for instance, that the FBI really needs a file on 30 million American citizens, one-third of the active labor force, in order to create an effective National Crime Information Center computerized criminal history system.

Currently, it actually plans to put one-third of the labor force in its NCIC file. I don't think that is needed; not even in New York do we think there are that many criminals.

Moreover, my colleagues in criminal justice are convinced that surely not one-third of the labor force is criminal in a way of interest to the FBI. Nevertheless, that is what the FBI plans. And I think that extension of data surveillance capability is unwarranted, absolutely unwarranted, by any concern about domestic security and crime.

Another trend is a major enhancement in the ability to merge information from segregated files through data base management techniques creating general purpose systems not authorized by Congress.

I think that 200 or so matching programs, described by Bob Smith and many others, being carried out at the Federal level, are nothing but primitive applications of data base technology. The essential purpose of data base management technology is precisely to merge information collected in one area of the organization and put it to work in another area of the organization. That is what we started out 10 years ago designing and that is what we have succeeded marvelously in designing.

In the private sector this is probably the single most significant technical advancement in computer technology. On the software side has been the whole concept of managing data, of data base management. Now, when it is applied to the public sector we run into real problems, however.

Congress, whenever it is given the opportunity to vote yes or no on creating a general purpose data base system like the National Data Center in 1968, or the Fednet in 1972, has rejected these systems as an unwarranted threat to the constitutional rights of American citizens. Nevertheless, matching programs are just inefficient, old style data base management technology. Instead of creating a single data base in which the data elements are precisely defined and available to thousands of programmers who surround the data base, as we would in a modern corporation—instead, the executive branch is creating ad hoc matching links between traditional data bases 1 to 1, until we have a patchwork of links which creates what I would call a shadow data base environment. It is one that is informally defined, it is ad hoc, it is inefficient, but it performs the same function as a data base management system.

This matching technology is creating systems and linkages which are far more complex than this Government or this society has dealt with in the past. Now, for reasons of efficiency in the administration of data, and for reasons of program efficiency and effectiveness, it may just be desirable to build these systems. But powerful checks and balances and oversight mechanisms must also be installed to assure the accountability of these systems to Congress.

There are many other troubling aspects that I have run across in the last 5 years working on national information systems. I have found a keen lack of concern for due process infringements created by poor record quality. Record quality is sort of a mundane issue that generally causes people to yawn.

But in a single FBI system, the National Crime Information Center and the Identification Division, I found a 22-million person record file in which 75 percent of the records had major errors and ambiguities and incompletenesses. I think that is astounding.

In another smaller sample of a Social Security file system for the Supplemental Security Income Program [SSI], I found over 25 percent of the case records had major errors of fact and of financial information on them.

And there is in the agencies, in my experience, a general lack of concern for the magnitude of these problems. When one converts from manual systems to automated systems, there is a keen lack of understanding of the significance of that; going from a manual environment where we have many, many errors in the underlying records to an automated environment where we are making hundreds of thousands of decisions per second, affecting people's lives radically. People are not recognizing that we had better do something about that data base and clean it up—they don't have that attitude.

It is a mundane issue, data quality, but it goes to the heart of the matter, which is how are we going to treat citizens in automated systems? If we get off into the technology side of the computer age, how many chips can we get per square centimeter? And we get onto the people side of the computer age, and the people side are questions such as how will we treat people? How will we treat errors? What kinds of correction mechanisms do we have? There isn't that concern in the agencies.

I have also found a lack of understanding of how equity and fairness can be built into systems, an unwillingness on the part of

agencies to allow citizens the use of technical means and devices to find out how agencies are treating their cases, for instance. Technology is applied, in other words, in a very one-sided way, from a management perspective—managing a caseload as opposed to a personal perspective, where we would like to get access to agency data.

The last trend I have noticed is the inability to conform to existing law and regulation to assure the accountability of systems to managers and to Congress. I have noticed this in the IRS and the FBI systems that I have worked on in particular, a desire to rush ahead to build systems before we have the regulatory apparatus established, and that bothers me.

It means that we have systems operating now, and will shortly, systems operating beyond the law.

Now, I have come to the general conclusion that it is not the technology per se that is the villain, the technology can't be separated from its uses. It is a little silly to talk about nuclear technology, for instance, without talking about the bomb. Nevertheless, the principal problem is having the courage and making the investment to learn how to control and regulate the technology to assure it can be held accountable to us.

Now, in the seventies we made a start at that with the Privacy Act of 1974 and the related family of legislation. But since then changes in technology have made that positive start technologically obsolete.

Since 1974, we have developed microcomputers that can sit on this desk top, as powerful as the main frame computers I used as a graduate student in the mid-1960's. Within 5 years, I can put on this desk a computer equal in capability to a good sized mini computer today. In a decade I can put the Library of Congress on this desk and give you the connections to speak to other libraries of the world in the giga bit range, that is in the billions of bits per second range of telecommunications.

That is how much the technology has changed in 10 years and will change in the next 10 years.

Now, along with that change, the appetite of large bureaucracies, both public and private, has clearly been stimulated. There is no longer a meaningful distinction between physical surveillance, electronic surveillance, and data surveillance.

You give me the right telephone numbers, a few of my graduate students, my IBM XT personal computer, and I will tell you where many of you were last night. In a few hours I can find out some very interesting details about your military, medical, Social Security, and employment records.

Now, if I can do that with a reasonably modest computer that operates at far less than a million instructions per second, these capabilities are clearly available to most large public bureaucracies and private organizations as well.

Mr. KASTENMEIER. May I interrupt to see if I understand you? [Laughter.]

On what basis would you have access to that information?

Mr. LAUDON. I asked you for the telephone numbers. I said if you give me the telephone numbers. It would take me a few hours of observation to find out the telephone numbers myself. But if you

could give me the telephone numbers, it would only take me a few hours to generate the codes of access to the systems in order to get that information. I would need a computer here in a few hours, though, to run through the combination of codes.

What right of access? The point is that it could be done without any formal right of access. The systems are that old.

Mr. KASTENMEIER. Would that be considered a theft?

Mr. LAUDON. Yes, a diversion of services and illegal entry.

Mr. KASTENMEIER. But you earlier indicated that there are many people managing systems that are actually operating outside the law in that connection.

Mr. LAUDON. I think there are some public sector Federal systems operating beyond the law, yes; right now. But my point was the breakdown between physical surveillance and data surveillance. With the right telephone numbers, in a few hours I can perform the same functions of physical surveillance of your person simply through data banks, simply because of the interconnections that exist between established data banks, and that capability is widespread. It is something that a few graduate students could do in an afternoon and, therefore, I assume that it is well within the means of IT&T or GE in a few hours to do the same thing.

So my point was not how easy it is to enter systems; my point was that the power of information in those systems is so great that people of modest capabilities, organizations of even modest capabilities, could put together in a few hours.

Mr. KASTENMEIER. Just to add to my understanding of computers and how they are operating in this connection, let me use a case in the graph here. We have a medical information system—we will assume it is a hospital and we will assume that voluntarily they provide an insurance company information because it seems legitimate. At a later point in time, the insurance company independently gives access to its computer system to a Federal agency, which the hospital had never intended to be a recipient of information about its patients. But for whatever reasons, the insurance company makes that information accessible to the third parties—

Mr. LAUDON. To the Social Security Administration.

Mr. KASTENMEIER [continuing]. To Social Security. Then really the ethical protection of information at the source is defeated because of remote and subsequent transactions.

Mr. LAUDON. To me one of the interesting aspects of the transaction you just highlighted is the extent to which we don't know that that already goes on. That particular transaction is which the Social Security Administration gains access to insurers' records having to do with a specific patient, is indeed a reasonably common transaction, because Social Security has a need for that information because it has to compensate the hospital often and it needs third-party insurance carrier information in order to do that.

There are a host of other transactions on this chart, the size and nature of which we are unsure. One of the points I very much wanted to make today was that the complexity of the data flows in the world is one of the major reasons why I think the information technology genie is out of the bottle. And significant improvements have to be made in the Privacy Act and related legislation in order to put the technology genie back where we had it.

In the particular case that you refer to, complex transactions between two and three, and perhaps four organizations, it is interesting to note that we don't have the expertise in our society to find out precisely how many of those kinds of transactions are going on.

Mr. KASTENMEIER. There is also another, I suppose, technical aspect. Some information may be available on a transitory basis from one system to another. And that may be qualitatively different if the recipient system downloads that information when the original system thought it was only available on a transitory, ephemeral basis. Retention and the development of additional data bases with sensitive information may also, I think, constitute a complicating fact.

Mr. LAUDON. It gets also more complicated if you mention downloading, if you consider downloading large files from a hospital to an insurance carrier, within the insurance carrier downloading that information to micro computers or small mini computers where it is worked on on small diskettes—what happens is eventually control is lost over the flow of that information, so that it becomes impossible to trace.

We ran into this problem and have continually run into the problem, at the IRS and at the FBI, trying to keep track of secondary and tertiary disseminations of data; trying to find out, and to answer the simple question: Who had what information at what point, when, and what did it look like? Can you trace this flow of information through organizations?

In many States, in certain areas like criminal records, they have given up. They basically tell State legislators and courts that we can't tell what happened to information once we sent it down to an agency, and it was subsequently disseminated within that agency. Now we would like to make a correction in the record. Maybe there was a mistake in the record, we would like to correct it.

Who do we talk to to correct that record? Who got it? Who made a judgment based on it that perhaps it should be corrected?

Well, here is an excellent example where we are operating technology beyond our management control, because we can't correct that record. If somebody lost a job because of a bad arrest on an arrest record in California, and we would like to rectify the situation, good luck; we can't do that. We are being forced to keep information on pieces of information. In order to keep track of information you have to know who had it, who saw it when. As it turns out that is more complicated than what we are willing to pay for. Therefore, we don't have those management capabilities.

That is an excellent example of what I mean when I say we are operating systems beyond our control and accountability. And I think Congress ought to be aware of that when it passes legislation which, for instance, asks us to build systems which can keep track of the flow of information for security reasons or for due process reasons. Building those systems is expensive and tends not to be done.

So the information could be sitting in a drawer somewhere, it could have been disseminated to a user somewhere, but nobody will know it. It could be on somebody's home micro computer, but nobody will know. There is no way of tracing that information currently, at least not in the way we build systems today.

I also want to point out in my testimony that there is literally only a handful of scholars in this country who work in this area. No major school of public administration can be of much assistance to you because they don't have any programs in national information systems, or even information systems. Only a handful of the business schools in this country have such major programs which would permit Congress to turn to an on-line group of experts for advice on how to build responsible systems. That expertise is not to be found in universities.

In my written testimony I called for a National Defense Information Systems Education and Research Act—one purpose of which is to help create the expertise in our schools of public administration.

I also called for a Privacy Protection Commission, just to give Americans a sense that some group has authority and interest in keeping track of these complex interactions among systems; in protecting their rights in the information age just as protect their consumer rights.

We need to amend in particular the "routine use" clause of the Privacy Act so that data surveillance can be more closely monitored. The routine use clause, with some of the strongest language in the Privacy Act, in which Congress specifically said that information collected for one purpose should not be used for another purpose unless specifically authorized by Congress. There was a very clear-cut statement.

There is no way, it seems to me, that that could be so misinterpreted, but it is, and has been for the last 10 years, by administrations on both sides. That clause, the routine use clause, has essentially been thrown out, and that opens up the whole Pandora's box of general purpose national information systems.

If that clause is not amended, then hearings such as this will, it seems to me, be irrelevant, because the gates will be open for a flood of systems based on the principles of modern data base management and technology, which is indeed to use information collected for one purpose to use it for another purpose.

Mr. KASTENMEIER. In your view, Professor Laudon, is that statutory language being misused or ignored, or does it in fact need to be amended to achieve the purpose you seek?

Mr. LAUDON. I don't have an answer to that question. I have fought with myself about ways that language could be strengthened, but it already seems to me so clear. And the willingness of the executive branch to abuse it seems to be simply a decision made by them and has nothing to do with the lack of clarity in the original legislation.

On the other hand, I would point out that that clause is so powerful, because it goes right to the heart of why we build systems. I mean, we build systems in the Federal Government, as in the private sector, in order to be efficient managers of data, and efficient users of data.

It does happen to be efficient to take information collected in one place and use it in another place. That happens to be in the private sector one of the major advantages of modern systems: the ability to transport information across organizational boundaries.

Therefore, the routine use clause makes a powerful statement. It says that the Federal Government will not avail itself of the most

advanced principle in the grab bag of data processing technology. We will forsake that efficiency in order to preserve a democratic republic.

That was a very courageous statement. I am not sure how maintainable that is going to be, and increasingly there is going to be a lot of pressure on that. The Privacy Act does say that you can have the most efficient taxation system in the world; within the IRS you can transfer all the information you want and you can use the most advanced technology, but you can't use tax data to support the Selective Service System, you can't do that. And that kind of efficiency we foresake, Congress said in 1974.

So the question you raise is can we go on? Can we be an efficient government without foresaking that routine use clause? And my answer to that is yes, we can, I think we can, I think we can design systems.

Now, there are going to be exceptions to routine use. The legislation in 1974 clearly says that Congress may authorize exceptions, and it did, the next day. It authorized the Parent Locator Service in 1974 to combine tax information and other information.

So there are certain circumstances under the right oversight mechanism where we will have to, perhaps, allow exceptions. Maybe the exceptions will grow in number; nevertheless, I will have some confidence if we have an oversight mechanism—a Privacy Protection Commission.

Mr. KASTENMEIER. In your view, we need oversight. Does the 1974 Privacy Act have any penalty clause associated with misuse or unauthorized use within the frame of reference of this statute?

Mr. LAUDON. Yes; it does have, but the penalties are rather minimal. It is a misdemeanor offense, I think, punishable by a thousand dollars or less, for abusing the Privacy Act. Of course, that only applies to Federal agencies; but many States have similar laws in the privacy area. But in general, one would say that—I have never in 10 years seen a prosecution at any level for a violation of the Privacy Act.

In conclusion, I can say that it seems to me that in the recent past, in the last 5 years, that we have tended to overestimate the gains in efficiency to be obtained by allowing information technology to have such a free rein. That has been my experience when you look at systems very closely. The FBI systems and IRS systems have been installed—some of those which are most objectionable in a civil liberties ground, are barely justifiable on a cost effective and cost efficiency basis.

Therefore, it has been disappointing for me at times—expecting great advances in efficiency, to find out that great costs in civil liberties had been incurred for very small advances in management efficiency.

I think there are alternative ways and alternative systems to achieving many of the same goals that the executive branch has outlined in its system development proposals.

I think we have to search for proper mechanisms for achieving those goals, and that we should not forsake our liberty out of fear for our security, or decrease our freedom in the pursuit of efficiency. I don't think we have to do that.

That concludes my testimony.

[The statement of Mr. Laudon follows:]

PREPARED STATEMENT OF PROF. KENNETH C. LAUDON, NEW YORK UNIVERSITY,
GRADUATE SCHOOL OF BUSINESS, COMPUTER APPLICATIONS AND INFORMATION SYSTEMS

My name is Kenneth C. Laudon. I am a sociologist and Professor in the Department of Computer Applications and Information Systems at the Graduate School of Business, New York University, where I teach on management information systems, and courses on the social and organizational impacts of information systems. I welcome this opportunity to testify before the Subcommittee on the question of civil liberties, security, and information technology.

I have worked in the area of information systems since the late 1960's when, with Alan Westin at Columbia University, I began a study of how third generation computers changed public decision making at state, local and federal levels. This resulted in a book entitled *Computers and Bureaucratic Reform*. Since this time I have participated as a consultant, researcher, and director in many of the major technology assessments concerned with information technology, organizational power, and civil liberties.

At the federal level I was a consultant to the Office of Technology Assessment's 1977 project on the Internal Revenue Service's Tax Administration System; in 1978 I was a member of the research group which examined the civil liberties implications of the Social Security Administration's proposed "Future Process" System. And, in 1979 I began a three year effort as a major contractor to the Office of Technology Assessment's study of the FBI's proposed national computerized criminal history system (CCH).

In a forthcoming book I have described my experiences with national information systems—especially the FBI's criminal history system. This book is titled "Security, Freedom, and Efficiency. Value Choices in the Design of National Information Systems."

I am delighted that you are interested in these subjects. In the hula hoop atmosphere which surrounds the marvelous technology of micro computers and integrated circuits it is frequently forgotten that the most important questions of the information age center about how people will be treated by information systems and the organizations which use them.

In my view, we, and members of Congress in particular have some difficult decisions to make about which values will reign supreme in the design of systems: international and domestic security, efficiency, or civil liberties. In my experience with specific national information systems, I found many aspects which were threatening to civil liberties:

—Major extensions in the data surveillance capability of central bureaucracies for minuscule gains in security and efficiency.

It is unclear to me, for instance, that the FBI really needs a file on 30 million criminals, one-third of the labor force, as opposed to a much smaller file on say a million serious criminals.

—Major enhancements in the ability to merge information from segregated files through data base management technology creating in some instances "general purpose" systems not authorized by Congress.

The 200 or so matching programs being carried out at the federal level are nothing but primitive applications of data base management technology in which information from diverse sources is pooled into a single "data base." Matching programs create shadow data bases. Yet, whenever Congress is given the opportunity to vote yes or no on general purpose data base systems like the National Data Center (1968) or the FEDNET (1972), Congress has rejected such systems.

A National Benefit System has been proposed by HHS several times in recent years, combining information on recipients of any federal aid—including college loans. In conjunction with a truly integrated Tax Information System which contained private market consumption data, a modernized social security system, and a fully capable national criminal history system, we would have the technical elements of a powerful surveillance apparatus.

These kinds of systems are only a few years off. They are far more powerful than anything this government or society has dealt with in the past. For reasons of efficiency in the administration of data, and for reasons of program efficiency and effectiveness, it may be desirable to build these systems. But powerful checks and balances and oversight mechanisms must also be installed to assure their accountability.

Other troubling aspects of some recent designs of national systems are:

—A lack of concern for due process infringements created by poor data quality

—A lack of understanding of how equity and fairness should or could be built into systems

—Inability to conform to existing law and regulation to assure the accountability of the system to managers and Congress.

I have come to the general conclusion that it is not computer technology per se which is the villain. Computer technology cannot of course be separated from its uses—any more than nuclear technology can be discussed without considering the bomb. Still, as with other technologies, the underlying problem is learning how to control and regulate the technology to assure its accountability to democratic institutions.

In the 1970's we made a start at controlling information technology in the Privacy Act of 1974—and related legislation. Since then, changes in technology have made this positive start technologically obsolete. Since 1984, we have developed micro computers that sit on a desk top which are as powerful as main frame computers I used as a graduate student in the 60's. In a few years, I can put on this table a computer equal in capability to today's large mini computers. In telecommunications we have gone from twisted copper wire, to optic fiber and satellites which transfer data in the mega and geiga bit range—that's millions and billions of bits per second. In a few years, we will put the Library of Congress on this table and connect you to most of the other libraries in the world.

Along with this technical change, the appetite of large bureaucracies—both public and private—for more and more data on individuals has also grown. There is no longer a meaningful distinction between physical surveillance, electronic surveillance, and data surveillance. Give me the right telephone numbers, a few of my graduate students, and my IBM XT personal computer and I will tell you where many of the members of the Subcommittee were last evening. In a few hours I could also find out a host of interesting details about your background—military records, medical, social security, employment, taxation, criminal and deviant behavior of you or any of your relatives. These capabilities are not lost on the large public bureaucracies—they are after all charged by Congress and the American public to give us efficiency, security, and effective administration.

The difficult question is this: in order to be maximally efficient, in order to protect against any and all foreign intelligence activity, in order to maximize the apprehension of domestic criminals, is it necessary to infringe on the traditionally defined civil liberties of Americans? To some extent this has already happened—few Americans have an expectation of privacy in foreign mails, telex, telephone or digital transmissions. Few knowledgeable Americans even have such expectations about domestic telecommunications—I don't. These rights have been sacrificed to national security—surely a laudable goal in itself.

In the 1970's we thought we had put the information technology genie in a bottle. The Privacy Act after all did have a very important clause—the routine use clause—which said in essence the federal government could develop whatever systems it wanted to within functional areas defined by Congress but it could not create general purpose information systems in which information collected for one purpose would be used for entirely different purposes. An efficient tax system was permitted, but not a system which merged tax information with Social Security data, Department of Defense Data, Veterans Data, and on and on.

The information technology genie is out of the bottle again and its time Congress takes another bipartisan look at how the federal government uses information technology.

In closing, let me say that I do not believe we can go backward in history or prevent the federal government from utilizing advance information technology. Neither must we sit idly by as our civil liberties are sacrificed. I believe we can have systems which are accountable to Congress, which advance not retard civil liberties, and which achieve high levels of efficiency and security. These systems are not easy to build, they are more expensive to design and operate, but they are appropriate to a democratic society.

In order to build these systems for the 1990's we need to encourage our graduate schools to train experts and conduct research on information systems and organization. It is ridiculous that no major school of public administration has a program in information systems, and only two or three major business schools have such a program. There is literally only a handful of scholars in this bountiful country who work in this area. We need a National Defense Information Systems Education and Research Act so that we have the expertise to answer the kinds of questions you and other members of Congress are raising today. We need a Privacy Protection

Commission just to give Americans a sense that some one group has authority and interest in protecting their rights in an information age just like we have agencies to protect us as consumers and to protect our environment. We need to amend the "routine use" clause of the Privacy Act so that data surveillance can be more closely monitored.

Above all we need to ask some tough questions of executive proposals for information systems. Is this system really needed or is it just icing on a bureaucratic cake, a proposal to preserve prior bureaucratic investments. Will it work and how well? Some systems upon examination offer minuscule gains in efficiency and security at great cost in public treasure and civil liberties. Are there alternative ways to achieve the same goals? And last, can the proposed system be held accountable to Congress and operate within existing law?

Without finding answers for these questions the preservation of our civil liberties will be left to technicians and bureaucrats concerned only with efficiency and security. As important as these goals are, so too is our liberty. After all, the idea of America in the beginning was freedom from surveillance and control so that we could be free to express, create, and live our lives. Let us not forsake liberty out of fear for our security or decrease our freedom in pursuit of efficiency.

Mr. KASTENMEIER. Thank you very much, Professor Laudon, for that excellent presentation.

When you say we need a National Defense Information Systems Education and Research Act, you are not talking about national defense in the military sense, I take it?

Mr. LAUDON. It seems to me, our national defense is threatened insofar as we, as citizens, are not exposed in any way to what an information system is.

This is an age of, unfortunately, computer literacy, in which people learn how to play with an Atari computer; that is very nice. And that is what our public schools, the most advanced public schools, are teaching right now. Even in our graduate schools we are teaching that to a broad array of undergraduates. We are all giving them microcomputers. That is well.

But there is a vast difference between a microcomputer and an information system, let alone a national information system. An information system involves large segments of organizations, they are infinitely more complex; they involve things such as how information gets into a computer in the first place; all of the information procedures, requirements and uses. Information systems are just incredibly more complex than a small computer.

So, therefore, I think a society that is moving into the information age ought to know something about information systems, which supposedly serve it. And that distinction between information system and a computer, unfortunately, is lost on most Americans, because our schools haven't really picked it up yet. We haven't paid enough attention to it. We don't have research programs in it; which is why it is so difficult, I think, to find experts to write about, and to monitor a large national information systems in either the public or private sector.

So I think our national defense is involved.

I could point to the Worldwide Military Command and Control System, which is known in the profession of computer processing, data processing people, as the world's largest mistake in the system. That is a \$5 billion national defense effort which was faulty in design from the beginning. We have given up on systems like that, in the private sector. Perhaps if we had had the right expertise there to chasten the Pentagon and to warn them of the failures that it was looking at, somebody might have saved them a lot

of money that they could have used elsewhere in the national defense.

The so-called WIMEX system stands out as perhaps a direct link between information systems knowledge and national defense.

Mr. KASTENMEIER. Information which I take it that because of pervasive data collection, the distinction of personal and sensitive people would traditionally consider a privilege in the legal sense and would naturally protect as a matter of privacy, is blurred. Computers and designers of computers really do not distinguish any longer what is personal and sensitive, they just collect everything they can collect on a person, notwithstanding the personal differences that might have existed at another time.

Mr. LAUDON. One of the things I didn't address in my testimony is the revolution in home telecommunications. We have cable companies, two-way cable companies, now offering shopping services and we have banks offering financial services, and soon we will have national tax preparation services offering tax preparation. And as the array of personal information services offered through PBX or ordinary telephone tie-ins, or cable, or satellite dish, as these services expand I think you are opening up the possibility that whatever information the consumer reveals by using these services takes on a monetary value and will be sold by the purveyor of those services.

So that you will be giving financial information to Chemical Bank or whatever your bank is; for instance, they may be paying all of your debts, you may have them pay your mortgage and your electrical bills, and book bills, and so forth. Pretty soon, that bank becomes the holder, not simply of your checking records, but also of all of your financial records that you clear through their system. And they can sell that information, just as two-way cable companies are now selling information on purchases that you make through the home through their two-way cable systems.

So that, indeed, as we become more reliant on these microcomputer based products and telecommunications products in the home, we open up new opportunities to reveal ourselves to outside organizations.

Some States have protections against that, but most States don't.

Mr. KASTENMEIER. Do you think that might be the subject of Federal legislation as long as some States do and some States don't? Would you have us make it uniform as a national question?

Mr. LAUDON. I think Congress ought to consider the possibility of a National Consumer Privacy Protection Act which would not necessarily be dependent upon cable technology and would, therefore, not necessarily be a piece of "cable" legislation but would be a part of a broader effort to protect the rights of Americans who interact with these systems as consumers.

Federal legislation isn't the only way that we can go. As we will hear from private industry, one of the things that could put a stop to a lot of the sales of data, certainly the sales of data to the IRS, would be if people found out that the IRS is indeed collecting this information, to refuse to participate; refuse to participate in home financial services; refuse to purchase things with your credit card.

Now, that kind of a movement wouldn't take much in certain circles to get started, perhaps a few well placed magazine articles rec-

ommending it as a strategy. In other words, I don't think that we have to rely on legislation only to protect our rights.

Another possibility is to consider attaching a cost to information by legislation, permitting people to charge for the uses of their names. Information obviously does have a value, there is no reason why we can't create a private market in it. We can create a private market in bundles of currency, we can certainly create markets in bundles of information and trade them in Kansas City. And all we have to do is attach a few cents per use for every use of my name, or any information to do with it, and have a national information clearinghouse established by Congress to take care of the check-clearing process at the end of the year. It is like a royalty statement. Instead of royalties, I would be paid for the uses of my name made in the year by any number of organizations, mail organizations, banks, manufacturers, so forth and so on.

So we could develop legislation which attaches a cost to information.

Mr. KASTENMEIER. It could also, of course, discourage that sort of collection?

Mr. LAUDON. Yes, yes.

Mr. KASTENMEIER. I want to thank you very much for your appearance here today, Professor Laudon. You have been very helpful to the committee and I hope you won't have as much difficulty getting back.

Mr. LAUDON. I hope not. Thank you.

Mr. KASTENMEIER. I would like to call as our next witness Mr. Alexander Hoffman, chairman of the board of directors of Direct Marketing Association.

I have asked Mr. Hoffman to appear before us today to discuss an issue brought to light in an article in the New York Times. The article reported that the IRS had asked the Direct Marketing Association to provide the Government with so-called lifestyles of persons with certain income levels suggested by marketing information collected from a variety of sources.

Mr. Hoffman is welcome here. I believe he has appeared before this committee in the past. He has been interested in copyright and publishing and many other worthy activities; he has been a patron of the arts in this community, and he has sponsored symposia with distinguished authors and others in which he has made a very substantial contribution. So we are very pleased to have you here, Mr. Hoffman.

TESTIMONY OF ALEXANDER C. HOFFMAN, CHAIRMAN, DIRECT MARKETING ASSOCIATION, INC.

Mr. HOFFMAN. Thank you. I appreciate the opportunity to testify before the committee on this very compelling subject.

I will be dealing with perhaps the more mundane side of it, the relatively simple use of information in mailing lists. I am going to try to truncate my written testimony since your counsel has suggested there are certain areas you perhaps would like to pursue with me in more detail. But I do think it is important to establish the fundamentals of how the commercial market in mailing lists

works as a piece of background information, so I will try to do that quickly.

The industry completely shares your concern to protect privacy. It is in our interest as well as the public's interest that that be done, because the whole system wouldn't work very well if the public lost confidence in it.

A little background quickly on how mailing lists work. A mailing list is simply a list of names and addresses which can be derived from sources as comprehensive as telephone directories or as selective as a subscription list to a small circulation magazine on contemporary art.

A retailer can maintain a list of his customers; a charity of its contributors, or a Congressman of his constituents. And each may, of course, attempt to categorize or segment them by, for example, product or service, frequency and type, or by party affiliation. The maintenance and storage is usually done by computer.

And in all cases, whatever the degree of refinement of the list, the objective is simply to ensure that recipients of mail sent out are likely to have an interest in what the mailer has to say. For example, when my company makes a mailing on behalf of the Literary Guild, we can only afford to mail to lists of that saving remnant of the population who actually read books, or at least are highly active readers in general who might become active book readers.

So what is the nature of the marketplace for these lists? It is common practice for a list owner, for example, a retailer with customers, a charity with donors, or a magazine with subscribers, to permit the one-time use of its list by another, frequently by an advertiser. For example, the Literary Guild might use the subscription lists of Harpers or the Atlantic Monthly for a promotion mailing because we know that readers of those magazines are above average book readers.

However, it is important to realize that a mailing list transaction prohibits the list user, by legally enforceable contractual obligation, from copying or making a record of the names and addresses on the list.

The purpose and the function of a mailing list is solely to furnish names and addresses to be used in the process of mailing promotional material of the user to the listed addresses. So typically the magnetic tape or mailing label list itself is delivered temporarily to an independent lettershop engaged by the advertiser or to the advertiser itself for the single mailing involved.

In the marketing world the list user never employs a list to ascertain any private information about any of the list members. He simply utilizes the list to get his mailing to the mailbox of potential customers who remain in effect anonymous so far as the list user is concerned.

So from all of this you can see that the process itself tends not to endanger personal privacy in any meaningful way—a conclusion which was reached by the Presidential Privacy Protection Study Commission in 1977.

However, let us look at the additional steps the direct marketing industry takes to ensure that privacy is protected. It is interesting

to note that they do these things in their own self-interest as well as in the public interest.

First, a mailer obviously has a strong economic incentive not to mail to people who find his mailings annoying and who throw them away unopened. To help reduce unwanted and hence unprofitable mailings, the DMA maintains the Mail Preference Service, which is widely promoted to the public.

MPS provides an individual with a means both to have his name removed from mailing lists or to have his name added to lists in which he may have a particular interest, for example, sports, camping equipment, books, or whatever.

Since the inception of this service in 1971, about 495,000 people have asked to have their names added to lists, while about 333,000 have asked to have their names removed. The add-on service was first offered in 1974, so that hasn't been running as long as the removal service.

Next, individual mailers notify their customers that they periodically rent their lists to others having something to offer in which they think their customers would be interested. But we give them the opportunity to have their names omitted from such lists if that is their desire. Thus, people can both get off of lists they are already on and avoid getting on lists in the first place, if that is what they wish.

Finally, the DMA has promulgated "Suggested Guidelines for Personal Information Protection," a copy of which is attached to this testimony, to provide individuals and organizations involved in direct mail and direct marketing with principles of conduct that are generally accepted and which will help ensure consumer privacy.

We believe they are routinely followed in the day-to-day operations of most of the business community.

The key to the whole process is the fact that direct marketers limit the collection and transfer of information to direct marketing purposes only. This has been the longstanding and natural practice of the business community inasmuch as it is only in these uses that the direct marketer has an interest.

By limiting the use of data to such commercially routine matters, consumer protection and privacy is not endangered.

Neither DMA nor the business community condones the use of mailing lists which are not compatible with the purpose for which the information is collected. Indeed, we believe this precept should be followed by all—government as well as the private sector.

The DMA guidelines specifically state that mailing lists should be rented for marketing purposes only, and we question the wisdom of Government agencies seeking to use them for other purposes. This would tend to undermine public confidence in a socially and economically important process, and possibly improperly invade personal privacy as well.

It is noteworthy that the U.S. Supreme Court has held that the first amendment protects not only a speaker's right to communicate, but also a listener's right to hear. Thus, when balancing the various delicate rights of individuals, the judiciary has fully protected all forms of commercial speech, including those uniquely employed by direct marketers.

Individual privacy is important to legitimate business people. With that in mind, the business community has done what we think is an effective job in seeing to it that consumer privacy is maintained.

I would be glad to pursue any of these things in more detail however you would like.

[The statement of Mr. Hoffman, and the guidelines, follow:]

STATEMENT PRESENTED BY ALEXANDER C. HOFFMAN ON BEHALF OF THE DIRECT MARKETING ASSOCIATION, INC., BEFORE THE HOUSE JUDICIARY SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE, WASHINGTON, DC, APRIL 5, 1984

My name is Alex Hoffman. I am Group Vice President of Doubleday & Company, Inc., a diversified New York publishing house which does general publishing, both hardcover and paperback, elementary and secondary textbook publishing, operates a chain of bookstores and runs a number of large and small book clubs.

I am here today as Chairman of the Board of Directors of the Direct Marketing Association, Inc., known as DMA, a trade association incorporated under the Not-For-Profit Corporation Law of the State of New York. On behalf of DMA, I extend my deep appreciation to Chairman Kastenmeier and the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice for the opportunity to share our thoughts with you today on the question of privacy protection.

I want to say at the outset that the direct marketing industry shares your concern that personal privacy continue to be protected in this era of the computer and other manifestations of high technology. My chief aim this morning is to help clarify the distinction between unauthorized release of properly private individual information and the legitimate, essentially anonymous use of marketing characteristics in compiled mailing lists—a process that serves the public well in many diverse ways.

DMA has nearly 2,400 member firms in 47 states and 26 foreign countries which represent every functional level of industry—manufacturing, wholesale and retail. These companies market goods and services through direct response methods, including direct mail advertising and mailing lists. As a measure of direct marketing's economic importance and consumer acceptance, consumer sales volume from catalogs alone was estimated to be \$44.4 billion in 1983, a figure that has doubled in only 7 years. We estimate that total sales volume of all direct marketing and related service industries approaches \$150 billion.

It is important to bear in mind the many and varied economic and social benefits of direct marketing. It is beyond the scope of this testimony to go into all of them, but suffice it to say here that direct marketing is an effective and efficient way to communicate information about available goods and services to targeted audiences, to provide maximum convenience to the elderly as well as to the increasing number of families with both heads of household working, and to aid fund raisers and charitable activities as well as to assist political candidates, parties and causes. Although mail is only one of the many media used to carry a direct marketer's message to his intended audience, it is convenient to use that medium as an example to demonstrate the methods which have been developed by the business community to protect consumer privacy.

First, a little background on the use of mailing lists in direct marketing. What is a list, where does it come from, and how is it used? A mailing list is simply a list of names and addresses which can be derived from sources as comprehensive as telephone directories or as selective as the subscription list of a small circulation magazine on contemporary art. A retailer may maintain a list of his customers, a charity of its contributors or a congressman of his constituents.

Each may, of course, attempt to categorize or segment them by, for example, product or service, frequency and type, or by party affiliation. Maintenance and storage is usually done by computer.

But in all cases, whatever the degree of refinement of the list, the objective is simply to insure that recipients of the mail sent out are likely to have an interest in what the mail has to say. For example, when my company makes a mailing on behalf of the Literary Guild, we can only afford to mail to lists of that saving remnant of the population who actually read books, or at least are highly active readers in general who might become active book readers.

What is the nature of the marketplace for lists? It is common practice for a list owner (e.g., a retailer with customers, a charity with donors or a magazine with sub-

scribers) to permit the one-time use of its list by another, frequently by an advertiser. For example, the Literary Guild might use the subscription list of Harpers or the Atlantic Monthly for a promotion mailing because readers of those magazines are above average book readers.

However, it is important to realize that a mailing list transaction prohibits the list user, by legally enforceable contractual obligation, from copying or making a record of the names and addresses on the list. The purpose and function of a mailing list is solely to furnish names and addresses to be used in the process of mailing promotional material of the user to the listed addresses. It is not to convey any information for any cognitive purposes and never purposely discloses anything beyond the name and address of each person on the list and, by implication, that he or she falls within the generic category of persons that comprise the list. Transposition of names and addresses from a list to the mailing pieces is done mechanically, electronically and automatically. A list user gains no information or knowledge as to the contents of the list by having the list, which in its physical form consists of magnetic tapes or sheets of labels, transmitted to him or received by him.

Thus, in many mailing list transactions (indeed, perhaps in by far the majority of them), the magnetic tape or mailing label list itself is delivered temporarily to an independent lettershop engaged by the advertiser, or to the advertiser itself, for the single mailing involved. In the marketing world, the list user never employs a list to ascertain any private information about any of the list's members. He simply utilizes the list to get his mailing to the mailbox of potential customers who remain, in effect, anonymous so far as the list user is concerned.

In these respects, a mailing list is a unique vehicle. It provides means for both mass communication and for individual attention; but the individual attention is provided to the listed person in the form of receiving something he is likely to be interested in, not by disclosing anything about him as an individual. To succeed, direct marketers must deliver their messages to the right prospects. A mailing list is the impersonal aid used to reach that goal.

From all of this you can see that the process itself tends not to endanger personal privacy in any meaningful way—a conclusion which was reached by the Presidential Privacy Protection Study Commission in 1977. However, let us look at the additional steps the direct marketing industry takes to insure that privacy is protected. It is interesting to note that they do these things in their own self interest as well as in the public interest.

First, a mailer obviously has a strong economic incentive not to mail to people who find his mailings annoying and who throw them away unopened. To help reduce unwanted and hence unprofitable mailings, the DMA maintains the Mail Preference Service (MPS), which is widely promoted to the public. MPS provides an individual with a means both to have his name removed from mailing lists or to have his name added to lists in which he may have a particular interest (i.e. sports, camping equipment, books, etc.). Since the inception of the service in 1971, about 495,000 people have asked to have their names added to lists, while about 333,000 have asked to have their names removed. The add-on service was offered in 1974.

Next, individual mailers notify their customers that they periodically rent their lists to others having something to offer in which they think their customers would be interested, and give them the opportunity to have their names omitted from such lists if that is their desire. Thus, people can both get off of lists they are already on and avoid getting on lists in the first place.

Finally, DMA has promulgated Suggested Guidelines for Personal Information Protection, a copy of which is attached to this testimony, to provide individuals and organizations involved in direct mail and direct marketing with principles of conduct that are generally accepted and which will help ensure consumer privacy. We believe they are routinely followed in the day-to-day operations of the business community.

It should be noted that no mailing list is conceivable that would be constructed on the basis of unfavorable information regarding the names upon it. Lists that constitute reports regarding the credit status of individuals are, of course, not mailing lists, and, in any event, they are already governed by the Fair Credit Reporting Act. The only consequence of being on a mailing list is that one receives something that he presumably has an interest in. At that point he is free to read it or throw it away as he chooses.

Key to the whole process is the fact that direct marketers limit the collection and transfer of information to direct marketing purposes only. This has been the longstanding and natural practice of the business community inasmuch as it is only in such uses that the direct marketer has an interest. By limiting the use of data to

such commercially routine matters, consumer protection and privacy is not endangered.

Neither DMA nor the business community condones uses of mailing lists which are not compatible with the purpose for which information is collected. Indeed, we believe this precept should be followed by all—government as well as the private sector. The DMA Guidelines specifically state that mailing lists should be rented for marketing purposes only, and we question the wisdom of government agencies seeking to use them for other purposes. This would tend to undermine public confidence in a socially and economically important process, and possibly improperly invade personal privacy as well.

It is noteworthy that the United States Supreme Court has held that the First Amendment protects not only a speaker's right to communicate, but also a listener's right to hear. Thus, when balancing the various delicate rights of individuals, the judiciary has fully protected all forms of commercial speech, including those uniquely employed by direct marketers.

Individual privacy is important to legitimate business people. With that in mind, the business community had done what we think is an effective job in seeing to it that consumer privacy is maintained. Should any questions concerning these matters arise, now or in the future, DMA will be pleased to offer its assistance.

The Direct Mail
Marketing Association's
Suggested
Guidelines for

**Personal
Information
Protection**

dm
ma

The Direct Mail/Marketing Association's Personal Information Protection Guidelines are intended to provide individuals and organizations involved in direct mail and direct marketing with principles of conduct that are generally accepted. These Guidelines reflect DMMA's long-standing regard for personal privacy and the responsibility of direct marketers to the consumer—a relationship that must be based on fair and just principles.

These Guidelines are also a part of the DMMA's general philosophy that self-regulatory measures are more desirable than governmental mandates whenever possible. Self-regulatory actions are more readily adaptable to changing techniques, economic and social conditions, and they encourage widespread use of sound and responsible business practices.

Because it is believed that a concern for everyone's privacy with respect to truly personal information is a basis for good business practices within direct response marketing, observance of these Guidelines by all concerned is recommended.

The Direct Mail/Marketing Association recognizes the need for businesses to protect the personal privacy of individuals and their need to provide safeguards for the proper handling of personal data contained in data files. DMMA strongly believes that good business practices require respect for such expectations of the individual.

Accordingly, DMMA recommends the following Guidelines for the handling of personal data in data files.

For purposes of these Guidelines, the following definitions apply:

Individual: A natural person identified in a file by name and address or other identifier.

Personal Data: Information which is linked to an individual on a file and which is not publicly available or observable.

Direct Marketing Purposes: The purposes of direct marketing are to promote, sell and deliver goods and services; to foster such efforts through the sale, rental, compilation or exchange of lists in accordance with the principles of these Guidelines; to delete and add individuals to lists; to provide all necessary customer services including the extension of credit where appropriate; to raise funds; to perform market research and to encourage recipients to respond by taking direct action.

Article 1. Personal data should be collected by fair and lawful means for a direct marketing purpose.

Article 2. Direct marketers should limit the collection of personal data to only those data which are deemed pertinent and necessary for a direct marketing purpose and should only be used accordingly.

Article 3. Personal data which are used for direct marketing purposes should be accurate, complete and should be kept up to date to the extent practicable by the direct marketer. Personal data should be retained no longer than is required for the purpose for which they are stored.

Article 4. An individual shall have the right to request whether personal data about him/her appear on a direct marketer's file and to receive a summary of the information within a reasonable time after the request is made. An individual has the right to challenge the accuracy of personal data relating to him/her. Personal data which are shown to be incorrect should be corrected.

Article 5. Personal data should be transferred between direct marketers only for direct marketing purposes. Every list owner who sells, exchanges or rents lists containing personal data should see to it that each individual on the list is informed of those practices (Self Disclosure), and should offer an option to have the individual's name deleted. The list owner should remove names from his/her lists when requested directly in a signed writing by the individual, or by use of the DMMA Mail Preference Service name removal list.

List brokers and compilers should take reasonable steps to have the list owner follow these list practices.

Personal data should not be put at the disposal of any third party except as set forth in these Guidelines, or with the express consent of the individual, unless required by law.

Article 6. All list owners, brokers and compilers should be protective of the individual's right to privacy and sensitive to the information collected on lists and subsequently considered for transfer.

Personal information supplied by individuals such as, but not limited to, medical, financial, insurance or court data

should not be included on lists that are rented or exchanged when there is a reasonable expectation by the individual that the information would be kept confidential.

Article 7. Each direct marketer should be responsible for the security of personal data. Strict measures should be taken to assure against unauthorized access, alteration or dissemination of personal data. Employees who have access to personal data should agree in advance to use those data only in an authorized manner.

Article 8. Visitors to areas where personal data are processed and stored should be specifically authorized by express permission of the direct marketer and should be accompanied by at least one authorized employee of the direct marketer.

Article 9. If personal data are transferred from one direct market to another for a direct marketing purpose, measures should be taken by the transferor to arrange strict security measures to assure that unauthorized access to the data is not likely during transfer procedures. It is the responsibility of the direct marketer to whom the list is transferred to arrange strict security measures to insure no unauthorized access to the list during its return to the original owner.

Article 10. The Committee on Ethical Business Practices of DMMA is charged with reviewing any complaints by individuals of violation of these Guidelines and shall take appropriate action.

DMMA Ethics Department

In its continuing efforts to improve the image of direct mail and direct marketing, DMMA sponsors several activities in its Ethics Department.

Ethical Guidelines are maintained, updated periodically and distributed to the field.

A Committee on Ethical Business Practices monitors the mails and direct offerings to the consumer and investigates complaints brought to its attention.

An Ethics Policy Committee initiates programs and projects directed toward improved ethical activity in the direct marketing area.

MOAL (Mail Order Action Line) handles consumer mail order complaints and MPS (Mail Preference Service) offers mail flow reduction or increased specialized mail to consumers.

All Ethics activities are directed by a full time Director of Ethical Practices.

For additional information contact:

John M. Cavanaugh
Director, Ethical Practices

Direct Mail/Marketing Association, Inc.
6 East 43rd Street, New York, NY 10017
(212) 689-4977

•
Suite 905, 1730 K Street, N.W.
Washington, DC 20006
(202) 347-1222

Members of DMMA proudly display this symbol and slogan:



"Look for this symbol when you buy direct."

Mr. KASTENMEIER. Thank you, Mr. Hoffman. The experience you have had, and the position of your association was very enlightening.

In refusing to cooperate with the Internal Revenue Service request for mailing lists reflecting certain levels of income, your organization, DMA, relied on its "Suggested Guidelines for Personal Information Protection." Now, these are admirable principles but they are guidelines, and just guidelines, which individual companies may choose to follow or not in any particular case.

I guess my question is: How do you react to whether or not the guidelines could be strengthened by legislative backing? If they were enacted into law, would that be a good development or would that be really an imposition on companies that might not want such Federal help? How do you respond to that?

Mr. HOFFMAN. That is a tough question. The natural instinctive reaction is to minimize further regulation, further legislation, but I think perhaps a case could be made.

We spoke at length with Rcscoe Egger, the Commissioner of Internal Revenue, about this, because we wanted to make sure that we understood fully exactly what they were trying to do and why. We are torn, because you cannot question the legitimacy of what the IRS is trying to do—they are trying to deal with the very intractable problem of finding what they estimate to be 5 to 6 million people who seek to be invisible and simply never file tax returns. That is a very tough nut to crack.

We simply wound up at the end of that meeting with a mutually understood difference of opinion.

What they are trying to do, they say, is find people, and they claim that they are only going to use lists based on public information. And they draw a distinction between lists compiled from public sources and lists compiled from private sector sources such as a company's customer list; but our concern is the public perception of this. The public will not be able, and will never make, fine distinctions between the sources of mailing lists. They will simply perceive that the Internal Revenue Service is using mailing lists to track people down. And in the minds of many of them they will say to harass them.

They will also come gradually to understand that the IRS is using census data to overlay on the basic mailing lists. And we believe that an inevitable consequence of such a chain of events carried out broadly and nationally would be a tendency on the part of people to view this as one more intrusion of privacy; one more step in Government intrusion into their lives; and they would gradually tend to conclude that it is not a very good idea to have your name on a mailing list. And next, perhaps, that it is not even a very good idea to be a voluntary participant in market research. And next, perhaps, that it is not even a very good idea to be a voluntary participant in filling out your census questionnaire.

These are subjective judgments as to what the consequences of the IRS action would be, but they tempt you to think that perhaps the principle of not using data for a purpose different from that for which it was collected, or that for which the person from whom it was collected expects it to be used, should be enforced.

Mr. KASTENMEIER. I guess that may answer my next question. I was going to ask you to clarify the point that you made that one of the reasons DMA is resisting the IRS request is that the expectation of privacy is essential to your business.

I assume you have just explained that. The perception is that the lists could be used for other purposes and it is harmful to your business in terms of making up lists.

Mr. HOFFMAN. I think the public understands perfectly well from their experience that up until now all that happens as the result of the existence of a mailing list is that you get mail. And you are either interested in it or you are not; you read it or you throw it away, and that is a perfectly benign process.

The expansion of this business is simply so staggering that it suggests that the public really does like it. I gave you some statistics in the part of the testimony I didn't read. But the total business volume of everything related to direct marketing now is approaching \$150 billion a year. The volume of business done just in catalog sales has doubled in less than 7 years. This catalog business is about \$44 billion or \$45 billion a year.

So this is a process that the public likes and they, at present, have confidence in it and accept it as a legitimate business process. But if they ever came to feel that endangerment of their personal privacy might become a byproduct of this, they could change their attitude entirely. So that is our concern.

Now, the Commissioner said to us, the public shouldn't think that way because it is in everybody's interest that we find these people who cheat, who never file tax returns; that hurts everybody, the public should wish to see that done, and they shouldn't feel threatened by the use of purely public sources of information in our efforts to do that. And that, taken in and of itself, is a perfectly true statement.

So then you get to the judgment of how the public will actually perceive it. And I have told you how we think inevitably they will tend to perceive it. They will not draw distinction between public and private sources for lists, but will just see the IRS using mailing lists to go after people, and perceive that as another invasion of privacy.

Mr. KASTENMEIER. Possibly a case could be made by the IRS, but the point is the person whose name is on the list really cannot determine how his name is to be used, whether for that reason alone or for other reasons. As the preceding witness suggested, an individual might sell his name and his information to anyone making up a list for other purposes. Obviously, I don't think that is feasible, but it does raise a point.

Mr. HOFFMAN. Let me make this concrete to show you why we think it is inevitable direct marketing would be harmed. When somebody joins the Literary Guild, in the welcoming letter that we send the new person, we say that we periodically make lists of our members available to other publishers and others who may have something to offer to you that we think you would be interested in, but if you prefer that we not do that, just say so and we won't, and we do exactly that.

Now, you would like to think that the member could accept that with confidence and believe exactly what we have said. But, if he

ever came to think that, instead of just renting that list to another publisher who might want to offer him books, somehow or other the Internal Revenue Service was going to get it, that is a whole other thing.

Mr. KASTENMEIER. Sure; you wouldn't contemplate that. In fact, there may be certain other publishers a person wouldn't like his name sent to, like Larry Flynt.

Mr. HOFFMAN. They have to trust our taste and judgment. We simply say at the outset that we exercise judgment, and we rent the list to people that we think you would like to hear from. They then exercise their own judgment as to whether our taste is acceptable or not, whether to trust me or not.

Mr. KASTENMEIER. This is very interesting because it does highlight a very specific issue even though it may be outside the norm of some of the abuses of privacy on other, more theoretical grounds. This is somewhat more narrowly business oriented; nonetheless, it is kin to the rest and has something to say about the society in which we live.

I appreciate your appearance here this morning, Mr. Hoffman. As I say, I think you have been before the committee in years past on different matters as a publisher, and we appreciate your contribution.

Mr. HOFFMAN. Thank you.

Mr. KASTENMEIER. Our last witness this morning is Prof. George B. Trubow of John Marshall Law School in Chicago IL, and director of the school's Center for Information Technology and Privacy Law.

Professor Trubow was general counsel for the Committee on the Right to Privacy under President Ford. He also served as deputy counsel to the Senate Judiciary Subcommittee on Improvements in Judicial Machinery.

Professor Trubow, we are pleased to welcome you this morning, and you may proceed as you wish, sir.

TESTIMONY OF GEORGE B. TRUBOW, PROFESSOR, THE JOHN MARSHALL LAW SCHOOL, CHICAGO, IL, AND DIRECTOR OF THE SCHOOL'S CENTER FOR INFORMATION TECHNOLOGY AND PRIVACY LAW

Mr. TRUBOW. Mr. Chairman, thank you very much. I appreciate the invitation to be here. I provided written testimony to the committee that is a general outline of answers to questions that you had put to me in your letter of inquiry and invitation. If I may, Mr. Chairman, I would ask that that be put in the record. What I would like to do is make some extemporaneous and supplementary comments today to flesh out that statement I prepared.

Mr. KASTENMEIER. Without objection, your 6-page statement will be received and made a part of the record in its entirety. We will be pleased to hear your oral statement.

Mr. TRUBOW. Thank you, sir.

Essentially I have three points to make to the committee. The first is that information technology being developed today is laying the foundation for a surveillance system and behavior control pro-

ess that George Orwell himself would have regarded as science fiction. It is coming, the foundation is being put in place.

Second, I want to make it clear that I am not speaking about unauthorized access to information nor the dissemination of wrong information. I am talking about threats arising from unrestricted access to correct information that has been voluntarily supplied for a legitimate purpose.

The warnings that have been given previously today by others with respect to unauthorized access, computer crime, and furnishing incorrect information, I believe are absolutely germane and those activities exacerbate a problem. The threat I focus on results from the use of correct information that originally had been voluntarily supplied by the data subject.

The third point is that time is running out and congressional action is about the only thing we can look to now for protection of personal privacy so that we do not in fact become subject to the incredible invasions of human dignity that Orwell predicted.

On the first point about the surveillance system both Bob Smith and Ken Laudon gave excellent testimony with respect to the vast information systems that are being developed. Separate data bases containing incredibly large quantities of sensitive personal information can be linked together. Communications technology makes it possible for us today, at the speed of light, to collect and exchange information for the various data bases in existence and being established.

Prior witnesses talked about Government file matching programs: the parent locator; the program whereby young men who have failed to register for the draft are found by file matching; the discovery of welfare cheats; the IRS file matching program to develop, of all things, a personal life-style profile of an individual resident or taxpayer so that the IRS can make decisions regarding the sufficiency of one's tax filing.

Bob Smith points out additionally, that credit bureaus are going to become a part of the day-to-day information exchange with the Federal Government. I think these are potentially frightening uses of information.

The previous witnesses have also told about additional activities of the Government to gather and use information. Mr. Chairman, you, yourself, know that in the last decade new information bases have been developed, new exchange of information is going on, and that has happened in the face of the Privacy Act of 1974, which had been passed to curtail that kind of activity. The act apparently has been ineffective in large measure from stopping that sort of conduct.

If we focus on the business sector for a moment, we can find that same kind of thing going on there but possibly even in a more frightening dimension. When I think of Big Brother, I don't think of Big Brother just in the person of the Government, because when we are talking about the marshalling and use of information, Big Brother can represent the private sector as well. Or it can be that person I am fond of talking about as, Little Brother next door, the neighbor who Professor Laudon mentioned has a personal computer in the living room or basement, and is able to participate in information networks.

New data bases are being established and linked all the time. I would like to concentrate on for a moment or two, as an example of what I consider to be the most significant kind of privacy threat, the electronic funds transfer system. That system now being developed throughout our financial community will provide the checkless, cashless society.

There are benefits and convenience that result from such a system; we don't have to carry around money, and we don't have to bother with checks that have to be written and circulated. How convenient to be able to use the EFT card at the point of sale where my purchase is instantly recorded, my account is debited and the account of the purveyor of goods or services is credited—all in an instant—at the speed of light.

As that system expands we find the basis for data surveillance that Professor Laudon talked about because we can have a minute-by-minute account of what someone is doing. As we live our day using that EFT card to buy our lunch, purchase a book, go to a movie, make reservations for the airlines, stay in a motel, all that can be recorded step by step.

All of those records could be maintained in a very, very specific form, with specific information available.

Most of us have already seen the front end of the EFT system at the grocery store when we carried our purchases to the optical scanner at the checkout counter. The uniform product code is read; and in some stores not only the monitor screen, but a voice tells us what we bought and how much we are being charged for it. We receive a very specific receipt that tells us not simply the price of an item but specifically what item we purchased. Those records will have to be kept in the system at least for audit purposes.

Think about how an individual can be profiled by his behavior, his whereabouts pinpointed at any moment of the day. Some credit document is not moving slowly through the mails; we are talking about information moving at the speed of light in networks throughout the country which can be instantaneously queried. That is the kind of system that is being established in the private sector.

I sometimes worry about what that means in terms of civil liberties from another standpoint: I think about those instances when someone has been denied credit, because of credit history, or error. Whatever that reason may be, somebody chose not to provide credit.

I think about the possibility that an individual, because of the EFT system, can be immobilized in society because his EFT card is not being recognized; his number, and as a result, almost his personality, is invalidated. His card won't be accepted by the system, for whatever reason.

We are talking about invasions of privacy, Mr. Chairman, that can result because an individual may have profiles and dossiers developed about him; because he is using systems that identify him, his behavior can be controlled while he moves through society and, indeed, he can be virtually immobilized in a crowd.

The result of all this is, that in fact we are developing a virtual central data base. The question of a national identity card or a single identifying number is growing moot. The linkages of infor-

mation systems, the networking of information in distributed data bases that can be instantly queried from any computer any place, makes a central data base a moot question, because we can get information wherever it is.

Because of the available personal identifiers, credit card number, social security number, name, address, other identifiers, a single identifier becomes less and less necessary. Technology is providing ways to link identifiers and files, Mr. Chairman. Something must be done now to protect the individual's privacy.

Where can we look for help? Let's look at the current administration. In addition to those file matching programs which are now in place, let's look at some other indicator's.

The administration wanted to have polygraph examinations of people in high levels of the executive agencies—and polygraphs, can be unreliable and intrusive forms of privacy invasion. The administration was pushing proposals from the FBI to use the National Crime Information Center, to keep an eye on people who had not committed a crime but are people who might associate with people with whom the FBI has an interest.

The administration wants to restrict FOIA inquires and Privacy Act privileges. This administration has withdrawn Executive orders previously issued by the White House which undertook to protect information and to restrict access of the White House to Federal information files.

A committee of the House, Mr. Chairman, the Government Operations Committee, did a study a while ago on Privacy Act implementation. It was reported that the OMB has been doing a poor job in keeping track of the implementation of the Privacy Act. There isn't very much interest in this administration to see how well the Privacy Act of 1974 is being implemented. And since 1974, there has not been a wide inquiry on Federal information systems.

What have the Federal courts been doing with respect to privacy? First of all, in the *Miller* decision, the Supreme Court told us that individuals do not have an expectation of privacy in their financial records; they don't even have standing to complain about it, said the Supreme Court. So the Congress had to step in and enact the Financial Privacy Act of 1978.

In the *Stanford* case, the Supreme Court thought it was all right for the files of newspapers to be searched by Government agents without process. And, again, the Congress had to pass the Privacy Act of 1980 to undo that and to provide some protection to the media.

The *Smith* case, involved the pen register, the device by which numbers called on the telephone are recorded—the Supreme Court said an individual has no privacy rights about the listing of telephone numbers called.

In *Paul v. Davis*, the Supreme Court said that information privacy is not protected under the Constitution, and it shielded from liability a State police official who distributed wrong criminal information about an individual.

That the current administration is not doing anything to forward the interests of individual privacy.

We cannot expect the Court to change its mind. It appears to me, Mr. Chairman, we must look to the Congress.

There has been some excellent work on information and privacy by the Office of Technology Assessment. I know that your committee has made an inquiry to OTA with respect to an assessment regarding questions of technology and Government data banks today.

I recommend such a study. Further, I earnestly recommend the establishment of some sort of Federal entity to do what the Privacy Protection Study Commission could not continue to do because it went out of business.

The current administration wants deregulation. I make a sharp distinction between deregulation that will stimulate the private sector economically and de-regulation in terms of protecting the liberty of individuals. Deregulation, to me, does not mean the protection of personal freedom. What it means to me is that protections for the freedom of individuals are being removed.

As much as I dislike levels of bureaucratic overlay, the average consumer today is unorganized and doesn't have a way of expressing a constituency, and never will have because of the diverse perspectives and interest of various individuals. It requires some institution. I believe, to look out for the individual's privacy.

I earnestly hope that you, your committee, and the Congress, will exercise leadership in assessing the situation and in establishing a mechanism that can protect the privacy that is slipping away.

I am reminded how appropriate your hearings are at this particular time. In the book 1984, that it was on April 4, that Winston Smith wrote, "Down with Big Brother."

This is a perfect time to begin examining how we can control the technology and control information systems, so that individual integrity can be protected. The dignity of the individual is one of the most important civil liberties in the world today.

I thank you, Mr. Chairman. I am willing to answer any questions you have now or may submit later in writing.

[The statement of Mr. Trubow follows:]

TESTIMONY BEFORE THE U.S. HOUSE OF REPRESENTATIVES, JUDICIARY SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES AND THE ADMINISTRATION OF JUSTICE, APRIL 5, 1984, BY GEORGE B. TRUBOW, PROFESSOR OF LAW AND DIRECTOR, CENTER FOR INFORMATION TECHNOLOGY AND PRIVACY LAW, THE JOHN MARSHALL LAW SCHOOL, CHICAGO, IL

Mr. Chairman, I am George B. Trubow, Professor at The John Marshall Law School of Chicago, Illinois, and Director of the School's Center for Information Technology and Privacy Law. Previously I have served as deputy counsel to the U.S. Senate Judiciary Subcommittee on Improvements in Judicial Machinery, Executive Director of the Maryland Governor's Commission on the Administration of Justice, and Director of Inspection and Review for the Law Enforcement Assistance Administration of the U.S. Department of Justice. From 1974 to 1976, I was general counsel to the Committee on the Right to Privacy, Executive Office of the President. I appreciate this opportunity to testify during your hearings on "1984: Civil Liberties and the National Security State."

Many people have celebrated the arrival of 1984, by noting that George Orwell's visions did not occur. There are no all-seeing two way television systems in our homes and offices to monitor our movements and thoughts, although information technology has come a long way since Orwell wrote his famous novel, "Nineteen Eight-Four."

Though Big Brother is not omnipresent as yet, perhaps the systems are now being developed that will monitor our every movement and examine our political, religious, business and social activities. The computer systems and networks being built now can provide the foundation for such surveillance as Orwell envisioned, even though he did not foresee the role that the digital computer would play in the future world.

Millions of home and business computers have already been sold and projections are that many millions more will be marketed in the near future. Information processes that were previously considered too small to justify automation can now be easily and cheaply converted to electronic manipulation. Attorneys, accountants, doctors, teachers, writers, and others are discovering that a great deal of their work can be performed on personal computers.

The information revolution goes far beyond the individual person processing information alone at home or in the office. The public and private data bases that are being developed and linked are a major part of the information revolution. These linkages come with a myriad of "hi-tech" names: Teletext, Videotex, Electronic Funds Transfer, The Source, Arpanet, and many, many more. Such systems will be the connection between millions of home, business, and government computers and centralized data bases. These "information highways" also provide the means for whomever owns them—government or business—to monitor and possibly to influence or control our movements, transactions and even our thoughts.

Teletext is the one-way transmission of information from a data base to a home computer which stores the information until the subscriber is ready to read it. Teletext is often compared to an electronic newspaper. Videotex is a two-way system that permits subscribers to query data bases for specific information, or to supply information themselves. While neither of these systems are widespread in the United States, as yet, they are being developed rapidly in Europe and can be expected to burgeon in this country, too. The obvious benefits from these new technologies, however, come with the inherent danger of loss of privacy. The information that flows through these highways, whether by telephone line or satellite, is subject to being monitored and copied. While the computer's vast memory capabilities and high speed operation creates the information revolution, it is precisely these same capacities that permit the monitoring of personal information and the surveillance of an individual's activities. For instance, consider the Electronic Funds Transfer System, known as EFT, which is the banking industry's system for creating a checkless and cashless society. With this system the transfer of funds, whether the most mundane point-of-sale transaction such as a grocery purchase or the most complex international high-finance arrangement, would be accomplished through computer linkages that debit and credit financial accounts and develop a minute-by-minute record of one's existence.

Of course, these types of files have been kept for centuries—long before the invention of the computer. However, the old pen and paper systems afforded natural protection for information; because they were too bulky and unwieldy that information was not easily available. It was simply too tedious and too costly to search the records, copy and transmit information. Today, on the other hand, computer speed and memory coupled with high speed transmission and printing put this information at an investigator's fingertips.

Anyone who has applied for any type of financial credit, bank loan, mortgage or credit card, knows that he or she must reveal great deal of information, including name and address, social security number, the names of banks where that person has accounts, his or her income and place of employment, and a list of debts and assets. Many people may not realize that signing the application gives almost a total waiver of the right to informational privacy, allowing the bank or credit institution to gather or supply virtually unlimited personal information about the applicant. Because retail credit bureaus keep files on at least 150 million Americans, almost anyone who uses credit can be certain that some faceless organization has detailed personal information about him or her.

For individuals who have something embarrassing in their past such as a juvenile arrest record, history of psychiatric treatment, or some financial problem, the existence of these files is like a ticking time bomb. Release of such information could lead to public shame or perhaps a loss of job. But the focus of privacy concern should not be merely on those who have histories that they would prefer to hide; more importantly, privacy should focus on all of us who have something to protect, and that is personal and family dignity. Privacy is the privilege not to have one's life an open book, at the behest of others. Privacy is the privilege to determine what information about oneself is to be shared with others and for what purpose personal information will be used.

Of course, if individuals want to participate in the benefits of society and new technology, they must surrender some privacy. Walter Cronkite sums up this dilemma in his foreword to David Burnham's Book, "The Rise of the Computer State:" "Without the malign intent of any government system or would-be dictator our privacy is being invaded, and more and more of the experiences which should be solely

our own are finding their way into electronic files that the curious can scrutinize at a touch of a button.

"Edmund Burke warned us more than 200 years ago: "The true danger is when liberty is nibbled away, for expedients and by parts." If privacy is the freedom from unwarranted intrusion by others, then we can see this "nibbling for expedients" taking place constantly today. Consider, for example, some of the current "routine" activities of federal and state government regarding computer file matching and information exchange which include locating the whereabouts of parents who have skipped out on obligations to dependent children, finding young men who have failed to register for the draft, and identifying individuals who commit welfare fraud. Most recently, the Internal Revenue Service began matching government and private sector data bases for the purpose of developing taxpayer "personal lifestyle profiles" to verify the validity of tax returns. The government justifies such activities for the "expedient" of catching wrongdoers, and most would not contest that objective. But these surveillance activities—the use of information gathered for one purpose being used for another purpose without the data subject's knowledge—are being implemented without guidelines developed with the benefit of national examination and discussion to define the proper balance between the individual's interests and those of government.

Former U.S. Senator Sam Ervin, Jr., at a 1971 Senate hearing on federal data banks and the Bill of Rights, stated the privacy problem this way: "Once people start fearing the government, once they think they are under surveillance by the government, whether they are or not, they are likely to refrain from exercising the great rights incorporated in the First Amendment to make their minds and spirits free." In other words, the knowledge that we are being watched forces us to conform and to alter the way we behave. After a while, this conformity can become second nature, and at that point we have truly lost our privacy and our freedom, and George Orwell's prediction will have come to pass.

A number of disturbing trusts are becoming clear:

The Government—state and federal—clearly has the propensity to develop profiles and dossiers of citizens and to carefully scrutinize their behavior.

More and more data bases of personal information are being developed by countless entities in the public and private sector.

Information communication technology—the ability to link these distributed data bases in a vast network—provides in effect a "central" national data base of personal information.

Files and linkages are being constantly enlarged. The development of horizontal business conglomerates makes available to individual customers general merchandising, insurance, banking, investment, accounting and real estate brokerage services; legal and medical service soon may also be available at the department store. With all these services furnished under one "roof," a massive "cradle-to-grave" personal information file becomes reality. There has been discussion in Washington about the establishment of a national identity card—which could surely be the key to identifying and linking every personal information base in existence. (As an aside, it can be noted that to a large extent, the social security number and bank charge cards already provide a pervasive means for information linkage).

The Congress has not made a careful and systematic examination of government or private sector information practices since it passed the Privacy Act of 1974. Indeed, that act appears not to have curtailed the governmental sharing of personal information—something that was a clear objective of the legislation. The Privacy Protection Study Commission reported in 1977; few of its recommendations appear to have been implemented. This year—1984—is an appropriate time to undertake another look at the status of government and private sector information practices, and I earnestly hope that the Congress does so.

I believe that experience indicates that the individual consumer is without adequate privacy protection. I quote from the findings of the National Symposium on Personal Privacy and Information Technology, sponsored by the American Bar Association and the American Federation of Information Processing Societies in 1981: "The individual's informational privacy is relatively unprotected and will remain so unless an effective constituency is developed." because of the diverse interests of our nation's population an organized privacy constituency cannot be developed. A further recommendation of the Symposium is, "Some long-term mechanisms or institutions, public, private, or both, must be established to examine and develop informational privacy policy that balances governmental, societal and private interests." Though I dislike the ideal of more bureaucracy, I believe that it is time for the federal government to establish some mechanism for privacy vigilance before it is too late to do so. Information and communications technology advances at an astonish-

ing rate of speed, and without prompt action to assess and establish privacy constraints it may soon be too late for action to be effective in protecting privacy. I hope that you, Mr. Chairman, will provide leadership in bringing about a national re-examination of information practices and in supporting the establishment of a federal institution that has responsibility to guard informational privacy.

Thank you.

Mr. KASTENMEIER. Thank you, Professor Trubow, for that excellent statement.

I am primarily interested in your recommendations, but because of the fact that there is a vote on and the hour is late, I am not going to detain you or those others present. I was interested in your recommendations for a study or other congressional action consistent with your view that time is of the essence; that this is a pervasive problem; and that the administration and the courts cannot be relied upon to respond to the problem.

I think we might consider trying to develop that aspect of your recommendations. I would appreciate any information that you might submit to the committee to help us determine whether we should make changes to present statutes to make them more effective, or whether we should proceed with a study precedent to that.

Mr. TRUBOW. I would be pleased to do that, Mr. Chairman.

I think that Ken Laudon was absolutely correct in pointing to the routine use clause in the Privacy Act of 1974 as having been misused. I believe that the discretion that administrative agencies have now to get around it should be curtailed.

Mr. KASTENMEIER. Thank you very much, Mr. Trubow.

Mr. TRUBOW. Thank you very much.

Mr. KASTENMEIER. That concludes this morning's hearing on 1984. Until next week when the committee will again be in session, the committee stands adjourned.

[Whereupon, at 12:45 p.m., the subcommittee adjourned.]

No page
330

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

WEDNESDAY, SEPTEMBER 26, 1984

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, CIVIL LIBERTIES
AND THE ADMINISTRATION OF JUSTICE
OF THE COMMITTEE ON THE JUDICIARY,
Washington, DC.

The subcommittee met, pursuant to call, at 10:10 a.m., in room 2226, Rayburn House Office Building, Hon. Robert W. Kastenmeier (chairman of the subcommittee) presiding.

Present: Representatives Kastenmeier and Schroeder.

Staff present: Deborah Leavy, David W. Beier, counsel; Joseph V. Wolfe, association counsel; and Audrey K. Marcus, clerk.

Mr. KASTENMEIER. The committee will come to order.

This morning marks the conclusion of a series of subcommittee hearings entitled: "1984: Civil Liberties and the National Security State." These hearings began almost a year ago on the eve of the Orwellian year of 1984 with the purpose of taking stock of the state of civil liberties in the very year Orwell used to warn us of the dangers of letting our precious freedom slip away.

At the onset of these hearings, I expressed concern over a number of acts which I viewed as threats to civil liberties: an Executive order demanding lifetime prepublication clearance for public speeches and writings of hundreds of thousands of Federal employees; barring the press from covering the invasion of Grenada; classification and labeling of certain foreign-made films; denial of visas to foreign speakers on thinly veiled political grounds; and restrictions on academic and scientific research.

Our hearings this past year have explored these issues and more, including electronic surveillance and other threats to privacy imposed by emerging technologies. We began these hearings on an optimistic note; after all, Orwell's vision is still mere fantasy. But as I noted at the outset, he never really meant "1984" to be a prediction; it was intended as a warning.

The testimony we have heard over the past year will, I hope, serve the same purpose. For what we have learned is that our civil liberties are, indeed, in danger. The parade of horrors that prompted my initial concern may be only the tip of the iceberg.

Technology has outstripped existing law on electronic surveillance, leaving loopholes for wiretappers, public and private; the Securities Exchange Commission has asserted that it can license fi-

nancial publications; the Commerce Department has demanded that a travel agency turn over a list of travelers to Cuba; the IRS wants to buy lists of high-lifestyle individuals from direct mail companies; and the Treasury Department has asked that banks report in detail all foreign transactions over \$10,000.

We have heard testimony that computers, rather than the tele-screens of Orwell's fantasy, may be the most efficient means of electronic surveillance in the future. Bank records, credit card records, telephone records, insurance records all leave a computerized trail that can reveal almost as much about an individual as constant physical surveillance.

But even telescreens may be on the horizon. During the course of these hearings, I received an update of the Manual for U.S. Attorneys and I note with alarm that the Justice Department apparently considers video surveillance permissible with few safeguards.

The subcommittee's hearings have revealed an almost invisible drift toward the Orwellian nightmare. It is now our responsibility to respond. Therefore, I am today introducing the Electronic Surveillance Act of 1984, a comprehensive bill that addresses many of the problems with respect to electronic surveillance which have been identified in these hearings. I hope that the bill will serve as a study document in the 98th Congress and that it will get serious attention in the 99th Congress.

I also hope our witnesses this morning will help us develop solutions to other civil liberties problems as well.

We are very pleased to have with us this morning three very knowledgeable witnesses. Our first witness, John Shattuck, is vice president for government, community and public affairs for Harvard University. He recently assumed that position after 13 years with the American Civil Liberties Union, 8 of those years as director of the Washington legislative office. In that capacity, he appeared before this subcommittee and others on many occasions. We, of course, are very pleased to welcome you today in your debut in your new role.

Our second witness, Ronald Plessner, is well known as an expert on privacy issues. He served as general counsel to the U.S. Privacy Protection Study Commission and has considerable experience with the Freedom of Information Act and as an attorney at the Center for Responsive Law. Mr. Plessner is now a partner with the Washington, DC, law firm of Blum, Nash & Railsback.

Our final witness will be Ms. Mary C. Lawton, director of the Office of Intelligence Policy and Review at the Department of Justice. Ms. Lawton testified before us on the Foreign Intelligence Surveillance Act not so long ago and she has had a long and distinguished career of service in the Department through several administrations.

We are indeed very pleased to have you all here today. Without objection, your written statements will be made a part of the record and you may proceed as you wish. First, I will call on Mr. Shattuck.

TESTIMONY OF JOHN SHATTUCK, ESQ., VICE PRESIDENT FOR GOVERNMENT, COMMUNITY AND PUBLIC AFFAIRS FOR HARVARD UNIVERSITY; RONALD L. PLESSER, ESQ., BLUM, NASH & RAILSBACK, WASHINGTON, DC; AND MARY C. LAWTON, ESQ., DIRECTOR, OFFICE OF INTELLIGENCE POLICY AND REVIEW, DEPARTMENT OF JUSTICE

Mr. SHATTUCK. Thank you very much, Mr. Chairman. I am delighted, as always, to appear before your subcommittee. I am often asked in my new capacity at Harvard to give my instant opinion on subjects that I know not anywhere near enough about and I should say that I feel from time to time like Yogi Berra when he was asked what time it is. He answered: "You mean right now?"

I am pleased that in this particular case, I have had a great deal of experience in the subject before you and commend you for addressing it in such detail.

I have submitted a number of documents for the record, including—I would like to mention—most prominently, a draft report on the subject of "Federal Restrictions on the Free Flow of Academic Information and Ideas."¹ I should stress that I am appearing here today in my individual capacity, but I did want to bring to the subcommittee's attention what is very much the academic perspective on many of the secrecy subjects that you have been investigating, as set out in the draft report that I have provided to you.

I have been asked in my testimony to put into perspective some of the themes that other witnesses have been addressing and I am happy to try to do so and also to be prepared to answer any questions you may have concerning the bill, which I am delighted that you have introduced, as well as the draft report.

A central theme of these hearings has been the threat to civil liberties from increasingly broad claims of national security asserted by the President and other officials of the executive branch. These assertions have become especially sweeping during the current administration, as in the case of the news blackout of the Grenada invasion, the promulgation of a Presidential directive imposing lifetime censorship on Government employees, handling classified information, the use of export controls to limit publication of scientific research and many other examples brought out in these hearings.

While the current administration has been particularly active in making claims of national security to curtail civil liberties, its policies are the culmination of a long trend which began after World War II and accelerated during the Nixon administration. Nowhere is this more evident than in the areas of censorship and electronic surveillance. Here the Nixon administration stands out from other recent Presidencies only because of the fate of its principal; not because its policies presented a unique threat to civil liberties.

In fact, the development of a law of national security secrecy and surveillance and its steady erosion of the first and fourth amendments has accelerated in the post-Watergate era.

¹ "Federal Restrictions on the Free Flow of Academic Information and Ideas," *Journal of Higher Education* (January 1985), supra, p. 1542; "Computer Matching is a Serious Threat to Individual Rights," 27 *Communications of the ACM* 538 (June 1984), supra, p. 3103.

Until 1971, the national security secrecy system had been created and maintained by the executive branch alone. The only law establishing the system was a series of Executive orders issued by Presidents Truman, Eisenhower, Kennedy, and Nixon.

There were security clearances in many Government agencies and millions of pages of classified documents, but there was no systematic enforcement of secrecy and no stamp of approval by the courts or the Congress. In my view, all that began to change when the Nixon administration went to court in May 1971 to try to block the New York Times from publishing the Pentagon papers.

Although the case is widely regarded as a victory for freedom of the press, and indeed it was in its result, the *Pentagon Papers* litigation actually set in motion the development of a formal law of national security secrecy. In the Supreme Court decision in that case, the Court abandoned the longstanding limitation of prior restraints on publication to narrow wartime circumstances. The pivotal concurring opinions of Justices Stewart and White for the first time generalized the category of information subject to prior restraint and recognized the authority of Congress to legislate in this sensitive constitutional area.

After the dust had settled, the Nixon administration and its successors began to claim that the Pentagon papers decision had actually established two key principles in a new law of secrecy. First, that the Government can block publication of information if its disclosure will "surely result in direct, immediate and irreparable damage to the Nation," as Justice Stewart put it; and second, that if Congress passes a statute authorizing prior restraint, the standard for imposing Government controls over information can be even lower.

The cat was out of the bag and a succession of post-Watergate cases transformed it into a tiger with a ravenous appetite for the first amendment. The most spectacular prior restraints in the period after the *Pentagon Papers* decision involved former employees of the CIA whose writings the Government claimed the right to censor. The *Victor Marchetti* and *Frank Snepp* decisions established the legal principle that the CIA, and presumably other Government agencies as well, can bar a current or former employee from publishing, and I quote from the injunction: "any information or material relating to the agency, its activities or intelligence activities generally, either during or after the term of his or her employment without specific prior approval of the agency."

This new principle was based on the law of contract. If you worked for an agency that operates within the national security secrecy system, your employment contract obligates you to waive permanently your first amendment rights to speak and publish without prior restraint.

Closely paralleling the growth of contract secrecy was the development of a legal theory that certain information can be "born classified." In 1979, the Justice Department moved against the *Progressive* magazine in an effort to block it from publishing information that was already in the public domain. The *Progressive* case involved an article written about the hydrogen bomb based on information obtained by its author, Howard Morland, from studying government publications.

In its effort to obtain an injunction, the Government argued that information about atomic weapons is "born classified" and can be restricted under the Atomic Energy Act, whether or not its disclosure would meet the *Pentagon Papers* standard. Although the Government eventually abandoned the *Progressive* case when it became clear that the information in the article was not secret, the theory put forward by the Justice Department was that there are whole categories of dangerous information that are beyond the reach of the first amendment.

Three years later, in 1982, the Reagan administration began using this same theory in its well-publicized effort to persuade academic scientists to submit certain categories of research to the Government for clearance. The report I have attached to my statement provides an account of the pressures on academic freedom that are resulting from this practice in a wide variety of areas that go beyond national security.

Like the law of secrecy, the law of national security surveillance has evolved from bold Presidential assertions of power to an extensive authority set forth in decisions and congressional enactment. Every President since Franklin Roosevelt has claimed the power to conduct warrantless wiretapping of foreign governments, but it was the Nixon administration which put forward the most sweeping claims in this area and sought to have them approved by the courts.

In a series of cases beginning in 1969, the Nixon administration argued that it had an inherent power to disregard the fourth amendment warrant requirement whenever it conducted wiretaps or physical searches of persons or groups believed to be a threat to the national security.

In the first such case to reach the appellate level, this argument was rejected by a court of appeals and a unanimous Supreme Court in 1972. Like the *Pentagon Papers* decision, however, the Court's ruling in the national security wiretap case was also significant for what it did not decide. Since the wiretap at issue had been installed on a domestic organization with no connections to any foreign power, the court left open the possibility that warrantless surveillance of a person or a group with foreign ties would be legal.

The political turmoil in the Nixon White House obscured the steady development of a new law of national security surveillance. Taking its cue from the Supreme Court's 1972 wiretap decision, the law began to focus on the elusive concept of foreign agency. Since the Court had held that the fourth amendment only barred warrantless national security surveillance of domestic targets, suspected agents of a foreign power were presumed to be beyond its reach.

Ironically, this distinction established a legal rationale for much of the surveillance that had been condemned in the Nixon era. One example was the CIA's program of spying on the antiwar movement entitled "Operation CHAOS." This was a surveillance effort to ferret out links between the leaders of the peace movement and foreign governments. Although no such links were ever established, the program resulted in the creation of CIA files on more than 300,000 domestic activists participating in activities that had been under suspicion for having a foreign stimulus.

The Ford, Carter, and Reagan administrations have all claimed, in a series of Executive orders, that undefined foreign agent surveillance is beyond the reach of the fourth amendment. These Executive orders have been issued with much public fanfare proclaiming the rule of law over the intelligence abuses of the Watergate era.

At the same time, however, the orders have been broadly drafted to fit the needs of national security, regardless of their impact on civil liberties. The Reagan order represents the culmination of this process. It goes beyond the foreign agent approach of the Carter administration and authorizes the CIA to conduct general surveillance of anyone inside the United States who may be in possession of significant foreign intelligence, such as journalists or academics or businessmen returning from trips overseas.

It also authorizes the CIA to conduct undefined covert operations inside the United States so long as they are not, and I quote: "intended to influence the political process, public opinion, policies or the media." No secret abuses can occur under this order; everything is out in the open, all within the claim of a general foreign security loophole to the Constitution.

Now, Mr. Chairman, this is the background, I think, on the areas of law that you have had most interest in in your investigations of national security in 1984. I think what we see is that national security has become a very broad concept with very little definition. There have been some attempts on the part of the Congress, few attempts on the part of the courts and even fewer attempts on the part of the executive branch to limit its scope.

I think the ultimate effect of much of the law that has developed in this area has been to authorize a great deal of flexibility in the management of security practices in the national security area.

The result is that today we have greater secrecy, more censorship, a CIA with more domestic authority, an FBI with fewer restraints and a National Security Agency with broader power than we have ever had in our history.

What is most remarkable about all of this is that we seem to have drifted into a state of permanent emergency that has no immediate context. We do not know what the emergency is or how long it will last. We do not even have a clear understanding of its impact on our system of liberty since we have been conditioned to accept the view that the rule of law often requires individual liberty to yield to claims of security under certain limited circumstances.

In fact, we do not even think of ourselves as living in a state of emergency. On the contrary, we believe that a general suspension of liberty happens only in other countries. Take a typical example close to home. On October 16, 1970, Prime Minister Pierre Elliott Trudeau went on Canadian national television and declared a "state of insurrection" throughout Canada based on the kidnaping of a Canadian minister and a British consul by Quebec separatists.

Trudeau invoked the Canadian War Measures Act and authorized the national police in Canada to conduct predawn roundups of French Canadians suspects of associating with the separatists. Trudeau's emergency decree had the effect of temporarily suspending the Canadian Constitution.

Comparing the Canadian and American approaches to national security, the Canadian Attorney General, John Turner, made a wry comment after Trudeau lifted his emergency decree. He said:

In a certain sense, it is a credit to the civil liberties of a country that it has to invoke extraordinary powers to cope with a real emergency. Some countries have these powers at their disposal all the time.

I think the question, perhaps a central question in this hearing—in these hearings—is whether the United States is becoming such a country. Without clearly defining what we mean by national security, we have turned it into a talisman to ward off any evil that might befall us as a nation.

It is disturbing, but not surprising, therefore, that the current administration has turned the CIA loose to spy on Americans and conduct covert actions inside the United States, created a presumption that all Government information about foreign or military affairs can be withheld from the public, pardoned FBI officials who supervised criminal burglaries as heroes in the war against terrorism and mounted a campaign for official censorship of scientific research.

I think there is a simple question that we must ask ourselves as we look at these recent developments and the long history of national security maneuvers that preceded them, and that is, where does the Constitution fit into this field? National security, we must remember, is what protects us from our adversaries, but the Constitution and the Bill of Rights are what distinguish us from them.

The question, of course, is not just one of law. It may not even be one primarily of law. We must decide what we mean by national security and whether its protection should be allowed to blur our principle distinguishing features as a nation. "Liberty lies in the hearts of all men," Judge Learned Hand said in a famous speech delivered during a time of grave national danger in 1943. "When it dies there, no constitution, no law, no court can save it."

Judge Hand's speech echoed the warnings of the drafters of the Bill of Rights, and in the words of Thomas Paine, "Those who expect to reap the blessings of freedom must also undergo the fatigue of supporting it."

Now, a second theme which I just would very briefly like to touch on, Mr. Chairman, following my assignment to provide a perspective on what has come out in these hearings, is the relationship between technology and civil liberties, and more particularly, the steady erosion of legal protections of individual privacy under the pressure from new technologies of communication.

This theme has been amply explored by many witnesses and I will only briefly summarize what I regard as the principal areas where legal developments have lagged far behind technology. The fourth amendment is rooted in the law of physical property and has traditionally been applied to protect property holders and occupants against unreasonable physical intrusion by the Government.

Where no physical intrusion has occurred, almost by definition, the law has long assumed that no invasion of privacy has taken place. For example, the Supreme Court, until 1967, declined to find that wiretapping involved any cognizable privacy interest on the part of persons whose telephone communications were intercepted.

Rapid changes in communications technology today are making property-based privacy protections substantially obsolete. Let me just summarize in a few sentences the major areas in which legislative action is essential if the privacy of communications is to be protected.

First, in the area of telephone and computer communications, messages are protected against intentional overhearing, but not against other forms of interception. Second, the combining or matching of computer data banks containing unrelated personal files is virtually unregulated today, despite a Federal statute that supposedly prohibits the Government from using personal information for purposes other than those for which it was collected except under certain defined circumstances.

Third, the privacy of mail matter is protected to the extent that it is enclosed in a wrapper or envelope, but there are few protections for private messages sent by means of electronic mail.

Fourth, the privacy of personal communication collected by credit reporting companies has some statutory protection today, but personal information collected by interactive cable television companies about the viewing habits and consumer choices of subscribers is subject to little or no protection.

These are just a few of the many areas of rapidly changing communications technology where individual privacy receives little or no protection. The courts have shown no inclination to extend the fourth amendment in this direction without statutory guidance from the Congress and from State legislatures.

This subcommittee is to be commended for its wide ranging survey of this problem and for setting a large agenda for legislation to update the law of privacy protection in the age of electronic communications.

Thank you very much, Mr. Chairman. I would be happy at any point to answer your questions.

[The statement of Mr. Shattuck follows:]

STATEMENT OF JOHN SHATTUCK
VICE PRESIDENT, HARVARD UNIVERSITY

on

"1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE"

Mr. Chairman:

I am delighted to appear before the Subcommittee to express my views on the subject of "1984: Civil Liberties and The National Security State". I should state at the outset that I am appearing here as an individual and not on behalf of any institution or organization. My experience with the subject of this hearing extends back to 1971, when I became national staff counsel to the American Civil Liberties Union, specializing in litigation involving issues of privacy, secrecy and governmental surveillance. In 1976 I became national legislative director for the ACLU and continued my work on civil liberties issues involving national security in the context of federal legislation. In July 1984 I left the ACLU to accept the position of Vice President of Harvard University. At Harvard, the Office of Government, Community and Public Affairs has recently completed a draft report, under my direction, entitled, "Federal Restrictions on the Free Flow of Academic Information and Ideas," a copy of which is appended to my statement.

In my testimony this morning I have been asked to put into perspective some of the themes brought out by other witnesses during these important and far-reaching hearings. I am happy to try to do so, with the understanding that the Subcommittee may also wish to question me about the governmental restrictions on academic research that are set forth in the attached report. I am also delighted that the Chairman has introduced legislation to provide privacy protection for new electronic modes of communication, and I would be pleased to respond to questions about this subject as well.

1. National Security and Civil Liberties

A central theme of these hearings has been the threat to civil liberties from increasingly broad claims of national security asserted by the President and other officials of the executive branch. These assertions have become especially sweeping during the current Administration -- as in the case of the news blackout of the Grenada invasion, the promulgation of a presidential directive imposing lifetime censorship on government employees handling classified information, the use of export controls to limit the publication of scientific research, and many other examples brought out in these hearings. While the Reagan Administration has been particularly active in making claims of national security to curtail civil liberties, its policies are the culmination of a long trend which began after World War II and accelerated during the Nixon Administration.

Nowhere is this more evident than in the areas of censorship and electronic surveillance. Here the Nixon administration stands out from other recent presidencies only because of the fate of its principal, not because its policies presented a unique threat to civil liberties. In fact, the development of a law of national security secrecy and surveillance, and its steady erosion of the First and Fourth Amendments, has accelerated in the post-Watergate era.

Until 1971 the national security secrecy system had been created and maintained by the executive branch alone. The only law establishing the system was a series of executive orders issued by Presidents Truman, Eisenhower, Kennedy, and Nixon. There were security clearances and investigations in many government agencies, and millions of pages of classified documents. But there was no systematic enforce-

ment of secrecy and no stamp of approval by the courts or the Congress. All that began to change when the Nixon administration went to court in May 1971 to try to block the New York Times from publishing the Pentagon Papers. Although the case is widely regarded as a victory for freedom of the press, the Pentagon Papers litigation actually set in motion the development of a formal law of national security secrecy.

In its Pentagon Papers decision, the Supreme Court abandoned the longstanding limitation of prior restraints to narrow wartime circumstances. The pivotal concurring opinions of Justices Stewart and White for the first time generalized the category of information subject to prior restraint and recognized the authority of Congress to legislate in this sensitive constitutional territory. After the dust had settled, the Nixon administration and its successors began to claim that the Pentagon Papers decision had actually established two key principles in a new law of secrecy: first, that the government can block publication of information if its disclosure will "surely result in direct, immediate, and irreparable damage to the nation," as Justice Stewart put it; and second, that if Congress passes a statute authorizing prior restraint, the standard for obtaining an injunction to stop publication can be even lower.

The cat was out of the bag. A succession of post-Watergate cases transformed it into a tiger with a ravenous appetite for the First Amendment. The most spectacular prior restraints to be imposed in the period after the Pentagon Papers decision involved former employees of the CIA whose writings the government claimed the right to censor. The Victor Marchetti and Frank Snepp decisions established the legal

principle that the CIA, and presumably other government agencies as well, can bar a current or former employee from publishing "any information or material relating to the agency, its activities or intelligence activities generally, either during or after the term of [his or her] employment...without specific prior approval of the agency." This new principle was based on the law of contract--if you work for an agency that operates within the national security secrecy system, your employment contract obligates you to waive permanently your First Amendment rights to speak and publish without prior restraint.

Closely paralleling the growth of contract secrecy was the development of a legal theory that certain information can be "born classified." In 1979 the Justice Department moved against the Progressive magazine in an effort to block it from publishing information that was already in the public domain. The Progressive case involved an article written about the hydrogen bomb based on information obtained by its author, Howard Morland, from studying government publications. In its effort to obtain an injunction, the government argued that information about atomic weapons is "born classified" and can be restricted under the Atomic Energy Act whether or not its disclosure would meet the Pentagon Papers standard. Although the government eventually abandoned the Progressive case when it became clear that the information in Morland's article was not secret, the theory put forward by the Justice Department was that there are whole categories of "dangerous information" that are beyond the reach of the First Amendment.

Three years later, in 1982, the Reagan Administration began using this same theory in its well publicized effort to persuade academic scientists to submit certain categories of research plans to the government for clearance. The attached report provides an account of the pressures on academic freedom that are resulting from this practice.

Like the law of secrecy, the law of national security surveillance has evolved from bold presidential assertions of power to an extensive authority set forth in judicial decisions and congressional enactment. Every president since Franklin Roosevelt has claimed the power to conduct warrantless wiretapping of foreign governments. But it was the Nixon Administration which put forward the most sweeping claims in this area, and sought to have them approved by the courts.

In a series of cases beginning in 1969, the Nixon Administration argued that it had an inherent power to disregard the Fourth Amendment warrant requirement whenever it conducted wiretaps or physical searches of persons or groups believed to be a threat to the national security. In the first such case to reach the appellate level, this argument was rejected by both the Sixth Circuit Court of Appeals and a unanimous Supreme Court in 1972. Like the Pentagon Papers decision, however, the Court's ruling in the national security wiretap case was also significant for what it did not decide. Since the wiretap at issue had been installed on a domestic organization with no connections to any foreign power, the Court left open the possibility that warrantless surveillance of a person or group with "foreign ties" would be legal.

The political turmoil in the Nixon White House obscured the steady development of a new law of national security surveillance. Taking its cue from the Supreme Court's 1972 wiretap decision, the law began to focus on the elusive concept of "foreign agency." Since the Court had held that the Fourth Amendment only barred warrantless national security surveillance of domestic targets, suspected agents of a foreign power were presumed to be beyond its reach. Ironically, this distinction established a legal rationale for much of the surveillance that had been condemned in the Nixon era. One example was the CIA's program of spying on the anti-Vietnam War movement, "Operation CHAOS." This was a surveillance effort to ferret out links between the leaders of the peace movement and foreign governments. Although no such links were ever established, the program resulted in the creation of CIA files on more than 300,000 domestic activists participating in activities that had been under suspicion for having a foreign stimulus.

The Ford, Carter, and Reagan administrations have all claimed, in a series of executive orders, that undefined foreign agent surveillance is beyond the reach of the Fourth Amendment. These executive orders have been issued with much public fanfare proclaiming the "rule of law" over the "intelligence abuses" of the Watergate era. At the same time, however, the orders have been broadly drafted to fit the needs of national security, regardless of their impact on civil liberties. The Reagan order represents the culmination of this process. It goes far beyond the "foreign agent" approach of the Carter Administration and authorizes the CIA to conduct general surveillance of anyone inside the United States who may be in

possession of "significant foreign intelligence," such as journalists or academics or businessmen returning from trips overseas. It also authorizes the CIA to conduct undefined covert operations inside the United States so long as they are not "intended to influence the political process, public opinion, policies or the media." No secret abuses can occur under the Reagan order. Everything is out in the open, all within the claim of a general foreign security loophole to the Constitution.

National security is a ubiquitous concept that presidents have frequently invoked over the last three decades to insulate their actions from review. The law has not only been inadequate as a safeguard against overreaching claims of national security; it has become, especially since the Nixon presidency, a source of legitimacy for the view that definitions of national security should be left to the discretion of the executive branch. Over the last decade the courts and the Congress have increasingly been drawn into the conflict between security and liberty, but instead of defining and narrowing security claims by the executive branch, they have often ratified executive practices and insured them against legal challenge.

The ultimate effect of much law in this area has been to authorize discretion and flexibility in the management of security practices. The result is that today we have greater secrecy, more censorship, a CIA with more domestic authority, an FBI with fewer restraints, and a National Security Agency with broader power than we have ever had in our history. And all of these developments have taken place in the shadow of the Nixon presidency, after we thought we had struck down the abuses that produced Watergate. Ten years later, most Americans

are not aware of this continuing erosion of their individual liberties in the name of a dangerously expanding concept of national security.

What is most remarkable about all this is that we seem to have drifted into a state of permanent emergency that has no immediate context. We do not know what the emergency is or how long it will last. We do not even have a clear understanding of its impact on our system of liberty, since we have been conditioned to accept the view that the rule of law often requires individual liberty to yield to claims of security under certain limited circumstances. In fact, we do not even think of ourselves as living in a state of emergency. On the contrary, we believe that a general suspension of liberty happens only in other countries.

Take a typical example close to home. On October 16, 1970, Prime Minister Pierre Elliott Trudeau went on Canadian national television and declared a "state of insurrection" throughout Canada based on the kidnapping of a Canadian minister and a British consul by Quebec separatists. Trudeau invoked the Canadian War Measures Act and authorized the national police to conduct predawn roundups of French Canadians suspected of associating with the separatists. Trudeau's emergency decree had the effect of temporarily suspending the Canadian Constitution. Comparing the Canadian and American approaches to national security, the Canadian Attorney General, John Turner, made a wry comment after Trudeau lifted his emergency decree:

In a certain sense, it is a credit to the civil liberties of a country that it has to invoke extraordinary powers to cope with a real emergency. Some countries have these powers at their disposal all the time.

Is the United States becoming such a country? Without clearly defining what we mean by national security, we have turned it into a talisman to ward off any evil that might befall us as a nation. It is disturbing, but not surprising, therefore, that the current administration has turned the CIA loose to spy on Americans and conduct "covert actions" inside the U.S.; created a presumption that all government information about foreign or military affairs can be withheld from the public; pardoned FBI officials who supervised criminal burglaries as heroes in a war against terrorism; and mounted a campaign for official censorship of scientific research.

There is a simple question that we must ask ourselves as we look at these recent developments and the long history of national security maneuvers that preceded them: where does the Constitution fit in? National security is what protects us from our adversaries, but the Constitution and the Bill of Rights are what distinguish us from them. The question, of course, is not just one of law. We must decide what we mean by national security and whether its protection should be allowed to blur our principal distinguishing features as a nation. "Liberty lies in the hearts of all men," Judge Learned Hand said in a famous speech delivered during a time of grave national danger, in 1943. "When it dies there, no constitution, no law, no court can save it." Judge Hand's speech echoed the warnings of the drafters of the Bill of Rights that, in the words of Thomas Paine, "those who expect to reap the blessings of freedom must always undergo the fatigue of supporting it."

2. Technology and Civil Liberties

A second theme of these hearings has been the relationship between technology and civil liberties, and more particularly the steady erosion of legal protections of individual privacy under pressure from the new technologies of communication. This theme has been amply explored by many witnesses. I will only briefly summarize what I regard are the principal areas where legal developments have lagged far behind technology.

The Fourth Amendment is rooted in the law of physical property and has traditionally been applied to protect property holders and occupants against unreasonable physical intrusion by the government. Where no physical intrusion has occurred, almost by definition the law has long assumed that no invasion of privacy has taken place. For example, the Supreme Court until 1967 declined to find that wire-tapping involved any cognizable privacy interest on the part of persons whose telephone communications were intercepted.

Rapid changes in communications technology today are making property-based privacy protections substantially obsolete. Let me just summarize in a few sentences the major areas in which legislative action is essential if the privacy of communications is to be protected. First, in the area of telephone and computer communications, messages are protected against intentional "overhearing", but not against other forms of interception. Second, the combining or "matching" of computer data banks containing unrelated personal files is virtually unregulated, despite a federal statute that supposedly prohibits the federal government from using personal information for purposes other than those for which it was collected. (See attached

article on computer-matching.) Third, the privacy of mail matter is protected to the extent that it is enclosed in a wrapper or envelope, but there are few, if any, protections for private messages sent by means of electronic mail. Fourth, the privacy of personal information collected by credit reporting companies has some statutory protection, but personal information collected by interactive cable television companies about the viewing habits and consumer choices of subscribers is subject to little or no protection.

These are just a few of the many areas of rapidly changing communications technology where individual privacy receives little or no protection. The courts have shown no inclination to extend the Fourth Amendment in this direction without statutory guidance from the Congress. This Subcommittee is to be commended for its wide-ranging survey of this problem, and for setting a large agenda for legislation to update the law of privacy protection in the age of electronic communications.

Thank you for the opportunity to appear for the Subcommittee.

Mr. KASTENMEIER. Thank you, Mr. Shattuck. I think we will postpone the questions until we greet the other witnesses.

Now I would like to call on Mr. Plessner, if I may.

Mr. PLESSER. Thank you, Mr. Chairman. I am delighted to be in front of this particular subcommittee. The last major piece of privacy legislation enacted by the Congress aimed at privacy was the Right to Financial Privacy Act of 1978, which came out of this subcommittee. It is important to note that Government access to private-sector records is the most important issue to be considered in terms of technology and privacy. This subcommittee is very much in the right place to look at the fourth amendment and what protections, if any, it has for our society.

I have reviewed all of the testimony given to the subcommittee in this series of hearings, and I believe that three major themes become apparent. First is that openness and public knowledge of public events is an important safeguard for democracy and is a crucial factor in the development of scientific thought.

Second, technology has outstripped those laws that we do have to protect against invasions of personal privacy. Most significant among these is whether digital communications are subject to laws which restrict or prohibit wiretapping. This point was made abundantly clear by Dr. Willis Ware, former vice chairman of the Privacy Commission, to this committee.

I also believe that there is a third major theme which should be focused on, and that is Government access to information main-

tained by third parties. This concern is heightened as the result of modern computer and communications applications. This has enabled Government agencies to request a wider and wider range of very detailed data on individuals, not necessarily limited to foreign intelligence activities. I think this is a trend that can be seen across the board with almost every Government agency.

For example, the Department of the Treasury is seeking to require the reporting to the U.S. Treasury of all bank transactions involving foreign banking activities. Those requirements were contained in a Federal Register notice of several months ago. I am not sure if the Treasury Department is acting on that in terms of final regulations at this point, but it was, I think, an extremely widespread, wide-reaching recommendation that was only possible because of modern communications and storage techniques. Essentially every foreign transaction going through a U.S. bank would have to be reported to the U.S. Government without any floor or dollar limit. The Treasury Department contended that they could do that under existing legislation. That example, raises to me what some of the major gaps are in the current law in this area.

The Privacy Act and the Freedom of Information Act bear mention for really just a moment. The comparison of the two acts is very instructive. Mary Lawton and I have been talking about those two acts since 1972 and we probably grew up on panels debating those issues and I would be happy to have her view now some 14 years later, but I think that the Freedom of Information Act has been a tremendously effective act. I think there has been criticism about it, right or wrong, but it has had a tremendous impact.

No one can, I think, deny the impact of the Freedom of Information Act. There have been thousands of cases; there have been millions of documents released. Behavior patterns in Government agencies have been fundamentally changed because of the Freedom of Information Act. It is a very simple law with very simple standards that have required the courts to intervene. You may like the change or not like the change, but the change has occurred.

The Privacy Act is much different. There is really only one strong benefit to the Privacy Act, which is the disclosure requirement. Government agencies have to disclose systems of records. I feel fairly comfortable that right now there aren't too many information practices or systems of records that are secret in the U.S. Government and I think that that has been an important step forward.

Other than that, the kind of very detailed regulations and requirements enacted by the Privacy Act, have not been as effective as they should have been. It has become primarily a tool for Government employees, which is a valid reason, but I don't think it has had the kind of overreaching value that the Freedom of Information Act has. I bring that up in the context of these hearings because I think at least 1 day was given to the need for openness and information practices and activities and I believe it's important to emphasize how effective openness is to the whole process, rather than regulation or control.

In terms of collecting information from third parties, searches of the records of individuals are no longer limited by the word "reasonable," as envisioned by the framers of the Constitution. The

technology of computers has sanitized search and seizure. Match programs done by the U.S. Government, search information about individuals is the same way as if the Government agent broke into your house and rifled the papers. However, because it is done on computer, such matches were not restricted. There is no warrant required; there are no rules really that apply and there is—because it is all in the computer, in the technology, people don't look at it as an invasion. If a Government agent came into a house or went into a safe deposit box, there would be a whole different concern about it. But I think what the technology is doing is playing a trick on us because it is not really any different.

You may in the end say it is OK for it to happen, but we should know what is happening before our pockets get picked by a machine that we can't feel. Technology is the future of our society, but we as a society have the obligation to establish rules and look at the development of these new activities.

One of the interesting issues on technology is that there are new institutions in our society today that didn't exist 12 years ago, 14 years ago. There are electronic mail companies that simply didn't exist—the concept didn't exist 10 years ago. Even in 1978, when the Right to Financial Privacy Act was written, many of these institutions, cable operators, interactive cable operators, electronic mail, didn't exist and the rules have changed for them.

If a government agency wants to get access to mail in the U.S. Postal Service, they have to get a warrant. If they want to get access to electronic mail, they don't have to get a warrant; they can simply walk in and ask for it. If a company wants to resist, they can force a subpoena, but there is no standard to apply and there is no real case history or case law in what are the rights of a person who has information in electronic mail. There is a technological twist because if you put your letter in the mail, it goes through the mail and it is completed. The Postal Service has no record of who it came from, who it was sent to, nor do they know what the contents were. It kind of flows through the common carrier system and ceases to exist.

For electronic mail, the information is kept on a computer at the electronic mail company: Who it came from; who it went to; and often the contents are kept for a minimum of 3 months. Such a data base becomes a rich one for Government agencies. There have been litigated cases. Even in Wisconsin, there has been a litigation with the source, one of the big companies, where they have resisted this kind of activity of where the Federal Government has attempted to get access to electronic mail.

It is simply something that didn't exist a couple years ago. There are now problems that we have to consider.

The IRS is now also—and you have heard testimony here—collecting information from private list brokers for the identification of nonfilers from public record information. The concern is not so much their present activities, but the fact that these activities are subject to few, if any, controls.

There is nothing in the law to prevent them from using information obtained to do profiles which may then be used to identify underfilers. The authority used by IRS is a very general authority for

them to collect information and I believe, gone to an extreme, and there can be some real dangers.

It is interesting to note, as a footnote, that it looks like the IRS use of these lists is not being very productive. Such lists are not as accurate and as effective as they thought they would be. The problem may just simply die because of that, but I think it is those kinds of programs that have come to light in this subcommittee and there should be continuation of examination.

There is one thing I would like to say before I get to what I think I am here for. The greatest tragedy in U.S. privacy policy is that there is no one really looking at this in the Government and certainly not in the administration. Congressman English's subcommittee recently released a GAO report indicating that NTIA essentially had less than one employee in the last several years looking at privacy issues. The Justice Department's interest in privacy is simply in defending cases. There is no—as I have seen, and I am sure Ms. Lawton will indicate differently, but from what we see from the outside, there simply is no policymaking. It is simply reactive.

Office of Management and Budget has spent little, if any, time on privacy and the tragedy is that these issues are coming up with new technologies and no one is thinking about them or coming up with position papers or helping the development of policy and it then rests for people on the outside to make suggestions. This past summer, I participated in a program of the American Bar Association with several members of the staff of this committee, as well as other congressional committees, where these concerns and problems were discussed. Out of that came a set of recommendations which are now winding through the ABA process and hopefully we will have an official statement by February, but essentially, the recommendations of that session this summer was that there need to be, both on the executive branch level in Congress and in the private sector, an organized effort to raise and to look at these issues and to reach some kind of judgment on the technology issues that are facing us in the privacy issue.

In terms of specific suggestions, I believe title III in the aural communications problem cries out for solution. I assume that is solved by the legislation that you have introduced today and I suggest only that it should be less of a study piece and really an action for direction action because I think the record is fairly clear on the need for that change.

Mr. KASTENMEIER. May I just interrupt to say that statement was made, of course, with the notion that we have less than 2 weeks left of this Congress.

Mr. PLESSER. My comments are not to be interpreted that I think anything will be passed this term, but I think that it is a mature issue, even though it may be one that should be raised next year.

The Government access to private sector records just simply needs to be looked at again very closely. The changes in technologies has resulted in activities which really need to be reexamined. I think the rules under which Government agencies are operating are changing.

I am not talking necessarily even about the FISA kind of activities of the foreign intelligence surveillance and wiretaps. I am just

talking about the much broader use of computer and information technology by Social Security Administration, by HEW, by Health and Human Services, by all of the agencies that collect and use data.

It is also time to look at the enforcement of the Privacy Act. The Privacy Act depends too much upon the courts, with not enough arbitration or guidance or rulemaking activity and that there needs to be a look at that.

Finally, getting back to Government access issues, in terms of the electronic mail and access to nontraditional means, there needs to be some legislation and examination and on the mailing list issue, if the Government is going to continue to use private sector information for profiling, I think there should be some control on that.

Thank you.

[The statement of Mr. Plessner follows:]

Testimony of Ronald L. Plesser
Blum, Nash & Railsback

September 26, 1984

Mr. Chairman, members of the Subcommittee, my name is Ronald L. Plesser and I am a partner at the law firm of Blum, Nash & Railsback, Washington, D.C. I first became associated with information policy issues in 1972 when I became Director of the Freedom of Information Clearinghouse, a project of the Center for Study of Responsive Law. During that period of time, I litigated many cases under the Freedom of Information Act, several of which involved issues of access to records where personal privacy was a significant issue. I was General Counsel to the United States Privacy Protection Study Commission ("Privacy Commission") from 1975 through 1977. Since that time I have been in the private practice of law in Washington, D.C. representing a broad range of clients in the freedom of information, privacy and information technology areas. I have served as Co-Reporter to the Drafting Committee of the National Conference of Commissioners on Uniform State Laws in connection with the preparation of a Model Information Practices Code. In addition, I was a Consultant to the National Telecommunications and Information Administration in conjunction with their consideration of the Privacy Commission's recommendations during the Carter Administration. I have written and spoken frequently on privacy and The Privacy Act of 1974.

This morning I am pleased to appear before the Subcommittee to discuss hearing of this Committee concerning access to government information, privacy problems and possible enforcement mechanisms.

I have reviewed all of the testimony given to this subcommittee in this series of hearings and I believe that two major themes become apparent. First is that openness and public knowledge of public events is an important safeguard for democracy and is a crucial factor in the development of scientific thought. Second, technology has outstripped those laws that we do have to protect against invasion of personal privacy. Most significant among these is whether digital communications are subject to laws which restrict or prohibit wiretapping. This point was made abundantly clear by Dr. Willis Ware, former vice chair of the Privacy Commission. I also believe that there is a third major theme, which you should focus on. This is government access to information maintained by third parties. This concern is heightened as the result of modern computer and communications applications. This has enabled Government agency to request a wider and wider range of very detailed data on individuals. For example, the Department of Treasury is seeking to require the reporting to the U.S. Treasury of all bank transactions involving foreign banking transactions. 49 Fed. Reg. 13548. Another example is the widespread use of matching programs by government agencies.

First, I would like to discuss the importance of openness as an element of privacy protection and my concerns with the Privacy Act of 1974. The Privacy Act of 1974 and the 1974 Amendments to the Freedom of Information Act were adopted within months of each

other. After that, the similarities of these two statutes become more and more difficult to determine. The Freedom of Information Act is a relatively simple, straightforward statute which has been very effective in its goal of creating greater access to Government records. The Freedom of Information Act has created much controversy primarily because of its effectiveness. There have been literally thousands of cases and tens of thousands if not millions of pages of documents that have been released because of The Freedom of Information Act. The Privacy Act has no such history of enforcement. To the extent that it has worked and that the goals of Senator Sam Ervin, its author, have been obtained, has primarily been a result of the efforts of the few in Government who have doggedly sought to keep the Act enforced. Unfortunately, these efforts are often mitigated by a greater interest in efficiency, which is not always the friend of privacy, and by many who view the Privacy Act as nothing more than a complicated set of bureaucratic requirements.

The problem with the Privacy Act is two-fold. First, it is its own worst enemy. It is overly complex, overly bureaucratic and contains few effective enforcement mechanisms. It has been almost totally unavailable to most citizens because of the cumbersome and frustrating nature of its enforcement remedies. Those who have succeeded in using the Privacy Act as an effective tool have in most cases been Government employees who have doggedly persevered in connection with claims that they have

against the Government. Moreover, in two key instances the Act clearly defeats itself. One of the basic tenets of the Privacy Act is that it limits the disclosure of records from agency to agency and to outside persons. However, this rule is waived where a disclosure is deemed a "Routine Use" and published 30 days prior to disclosure in the Federal Register. This exemption swallows the whole. For example, the FBI allows public disclosure to agencies essentially if they have a good reason for it. (See Notice for Justice (FBI-002)). As a result of these interpretations there are effectively no limits on disclosure.

A second basic tenet is a person's ability to see and copy records about himself. The exemption structure of the Act exempts many agencies, including all of those with criminal law enforcement authority. Some problems lie with the courts and the Government in their collective failure to broadly interpret and actively enforce the provisions of the statute. The Justice Department in particular, has made the Act extremely difficult to use seeking any excuse to avoid judicial jurisdiction. There also has been a failure within the Government to monitor and evaluate the implementation of statutes and regulations related to privacy. There has been almost no research, study or investigation in areas of privacy on behalf of the Government. Moreover, the Government, OMB in particular, has done relatively little to issue interpretative rules or other guidance to assist agencies in connection with their enforcement of the Act. It is

my hope that the testimony in these hearings will create an atmosphere of re-evaluation for the concerns of privacy in the Federal Government.

The Privacy Act has had one extremely significant benefit. That is, its prohibition of the maintenance of secret systems. I suspect that there are very few systems of records of major significance which are not now disclosed by the Federal Government in at least some level of detail. This is a very beneficial effect for the public, for those of us who examine the Government and for the Government itself. Never, before the Privacy Act did the Government have anything approaching an index of the types of records that they maintain about individuals and why those systems have been maintained. The Privacy Act has been extraordinarily therapeutic in its examination and disclosure of what systems the Government maintains. Beyond that and beyond its assistance to the Government employees who have used it, it has been of comparatively minor effect.

I believe that an important theme, is access to bank records. In examining privacy in light of new technology, a review of the state of Fourth Amendment rights will help view the principles of privacy. This examination inevitably leads to the conclusion that the Constitution gives little, if any, protection to an individual and that we must look to legislative solutions, government mechanisms and Congressional oversight to protect the interests of privacy in our society.

The Privacy Commission's ability to conceptualize the problem it was trying to face in looking at an individual's right to control information maintained about individual's right to control information maintained about individuals was facilitated by a case entitled Miller v. U.S., 425 U.S. 435 (1976) issued by the Supreme Court in the midst of the Privacy Commission's deliberations. The Miller story still had two lessons which are still of importance. First, the Fourth Amendment probably cannot survive the technological age and, second, that only by the protection of the rights of those in contact with the law can we protect the rights of all. Mitchell Miller's story bears repeating. An agent from the U.S. Treasury Department's Bureau of Alcohol, Tobacco and Firearms suspected Miller of direct involvement in two events, a seized truck and a warehouse fire which indicated illegal manufacture of alcoholic products. Two weeks later, the agent presented grand jury subpoenas to the two banks where Miller maintained accounts. Without notifying Miller, copies of his checks and bank statements were either shown or given to the Treasury agents as soon as they presented the subpoenas. The subpoenas did not require immediate disclosure, but the bank officers nonetheless responded at once.

After he had been indicted, Miller attempted to persuade the court that the grand jury subpoenas used by the Treasury Department were invalid and, thus, the evidence obtained with them could not be used against him. He pointed out that the

subpoenas had not been issued by the grand jury itself, and further, that they were returnable on a day when the grand jury was not in session. Finally, Miller argued that the Bank Secrecy Act's requirement that banks maintain microfilm copies of checks for two years was an unconstitutional invasion of his Fourth Amendment rights. The trial court rejected Miller's arguments and he appealed.

The Fifth Circuit Court of Appeals also rejected Miller's claim that the Bank Secrecy Act was unconstitutional, an issue that had already been resolved by the U.S. Supreme Court in 1974. The Court of Appeals agreed, however, that Miller's rights, as well as the bank's, were threatened and that he should be afforded the right to legal process to challenge the validity of the grand jury subpoenas. The Court of Appeals saw Miller's interest in the bank's records as deriving from the Fourth Amendment protection against unreasonable searches and seizures which protected him against "compulsion production of a man's private papers to establish a criminal charge against him."

On April 21, 1976, a fateful day for personal privacy, the U.S. Supreme Court decided that Mitchell Miller had no legitimate "expectation of privacy" in his bank records and thus no protectible interest for the Court to consider. The Court reasoned that because checks are an independent record of an individual's participation in the flow of commerce, they cannot be considered confidential communications. The account record,

moreover, is the property of the bank, not of the individual account holder. Thus, according to the Court, Miller's expectation of privacy was neither legitimate, warranted, nor enforceable.

Since the Privacy Commission's report, the Congress principally through this subcommittee enacted the Right to Financial Privacy Act, which to a limited extent, gives depositors some standing to challenge Federally-issued subpoenas. The Supreme Court's conclusion that Miller could do nothing to protect records about him, however, has not changed. Individuals have less and less control over information maintained about them. The Constitutional protections of the Fourth amendment continue to be eroded and soon little will be left. This is now demonstrated by the activities of the Treasury Department in seeking the disclosure of all foreign bank transactions.

Searches of the records of individuals are no longer limited by the word reasonable as envisioned by the framers of the Constitution. The technology of computers have sanitized search and seizures. Match programs search information about individuals to the same end as if a government agent broke into your house and rifled your papers. But because you can't see it and because the ends are justifiable, the Fourth Amendment is deemed irrelevant. The Fourth Amendment is fast becoming a dead

principle in light of electronic mail and other potential areas of access to private information.

We are now also facing an increasing effort by the Treasury and IRS to travel further and further away from the principles of privacy set forth in the Tax Reform Act of 1976, the Privacy Act of 1974 and the Recommendations of the Privacy Commission.

The IRS is now also collecting information from private list brokers for the identification of nonfilers from public record information. The concern is not so much their present activities, but the fact that these activities are subject to few, if any, controls. There is nothing in the law to prevent them from using information obtained to do profiles which may then be used to identify under-filers.

The authority relied upon by the IRS in Section 760(a) of the Internal Revenue Code which states:

"The Secretary shall, to the extent he deems it practicable, cause officers or employees of the Treasury Department to proceed, from time to time, through each internal revenue district and inquire after and concerning all persons therein who may be liable to pay any internal revenue tax, and all persons owning or having the care and management of any objects with respect to which any tax is imposed."

This type of general authority does not effectively limit the collection practices of the IRS. Moreover, the IRS, disowns the source of the mailing lists and states that they are "generally" taken from public sector lists.

Without guidance, it can be expected that IRS will use private lists from private sources to identify potential underfilers. We believe that this is potentially a further invasion of a person's privacy and can lead to the connection of private sector information data bases.

All of these issues leads us to ask who in the Administration is looking at privacy and who if anyone is seeking to balance other governmental balance with those of privacy. The answer is that nobody is looking at privacy. The Privacy Commission recommended an alternative approach.

The Privacy Commission was directed by the Congress in the Privacy Act of 1974 to examine the effectiveness of the Privacy Act itself and to make recommendations concerning certain of its provisions. The Privacy Commission recommended significant revisions to the Privacy Act primarily aimed at the exemption structure, the availability of damage remedies and the system of record-routine use concerns. I think by and large the Privacy Commission's analysis of the Privacy Act in 1977 holds true today.

One of the recommendations of the Privacy Commission which has been often overlooked is one that I think bears repeating this morning and further examination in detail. The Commission stated:

"in all areas of the public sector the Commission has studied, the need for a mechanism to interpret both law and policies is clear. The difficulty of deciding which disclosure of

records about individuals are routine within the meaning of the Privacy Act often raises conflicts of interests or interpretation between two or more Federal agencies. Similarly as indicated in Chapter 13, Federal agencies often need an efficient means of arriving of common solutions to their common privacy protection problems such as establishing procedures for the disposal of records, the propagation of corrections and the maintenance of accounting disclosures".

(Privacy Commission Report, p. 36).

In furtherance of those conclusions, the Privacy Commission recommended:

"That the President and the Congress establish an independent entity within the Federal government charged with the responsibility of performing the following functions:

- (a) To monitor and evaluate the implementation of any statutes and regulations enacted pursuant to the recommendations of the Privacy Protection Study Commission, and have the authority to formally participate in any Federal administrative proceeding or process where the action being considered by another agency would have a material effect on the protection of personal privacy, either as the result of government regulation of others.
- (b) To continue to research, study, and investigate areas of privacy concern, and in particular, pursuant to the Commission's recommendations, if directed by Congress, to supplement other government mechanisms through which citizens could question the propriety of information collected and used by various segments of the public and private sector,
- (c) To issue interpretative rules that must be followed by Federal agencies in implementing the Privacy Act of 1974 or revisions of this Act as suggested by this Commission. These rules may deal with

procedural matters as well as the determination of what information must be available to individuals or the public at large, but in no instance shall it direct or suggest that information about an individual be withheld from individuals.

- (d) To advise the President and the Congress, government agencies, and, upon request, States, regarding the privacy implications of proposed Federal or State statutes or regulations.

(Privacy Commission Report, p. 36).

The entity the Commission recommended may be a Federal Privacy Board or some other independent unit. However, if a new entity is established, the only enforcement authority the Commission would recommend it be given would be in connection with the implementation by Federal agencies of the Privacy Act itself. Its oversight responsibility in all of the other areas covered by the Commission's recommendations would require it only to participate in the proceedings of other agencies when substantive privacy issues are involved. For example, if the Federal Reserve Board were to issue proposals which amend its regulation Z pursuant to the Truth-in-Lending Act after the Commission's recommendations are adopted, the new entity could participate in the proceedings only to the extent of presenting testimony and other comments from a privacy protection point of view.

Interestingly enough, it is Item (b) of the Privacy Commission proposals which most cries out for action. There is simply no independent board, body or person in the Federal

Government whose job it is to research, study and investigate areas of privacy. The Office of Management and Budget deals with the Privacy Act in order to make its application the least burdensome on agencies. They answer questions while they should be asking them. The National Telecommunications and Information Administration ("NTIA") had the job for a while of looking into information policy and privacy in particular. That function for NTIA has been all but eradicated. There is no agency to resolve issues such as match, to resolve the conflicts between the application of the Privacy and the Freedom of Information Act or the use of IRS data by agencies other than IRS. The Justice Department has taken on a role of representing its clients and not of developing policy. I believe that in the year of 1984, which will both be the ten year anniversary of the Privacy Act, and is a year of literary significance, Congress should consider the establishment of such a Commission for purposes of making the Privacy Act a realistic tool to protect individual rights.

Mr. KASTENMEIER. Thank you, Mr. Plesser.

Now I would like to call on Ms. Mary Lawton, counsel for Intelligence Policy of the Justice Department.

Ms. LAWTON. Thank you, Mr. Chairman.

I will not read the whole statement; you have it and have indicated it is going in the record, but there are a couple of points I would like to raise from it.

One is that our system is not antithetical to the concept of secrecy. We have always recognized twin values of openness and confidentiality. The Constitutional Convention that structured our Government with a value of openness met in secret. The Bill of Rights proposed by our First Congress reinforced twin goals of openness and confidentiality. Just two examples from the first amendment are that the free exercise clause allows an individual to hold religious beliefs in confidence without prying by the Government. The right of assembly creates, in some aspects and under some circumstances, a privacy right so that the Government cannot inquire into one's friends and associates. So that even in the first amendment, which protects free speech and openness and academic freedom, there is also an element of confidentiality, of secrecy.

Our legal tradition, likewise, recognizes both confidentiality and openness. Grand jury secrecy is accepted as a protection, not only of the individual, but of the legal process. Our Rules of Evidence recognize the importance of protecting confidential relationships in a privileged context and this includes the State's secrets privilege protecting diplomatic and military information in the interest of national security.

Congress has created expectations of confidentiality and indeed mandated secrecy with criminal sanctions. I am not referring only to the Espionage and Atomic Energy Acts, but there are criminal penalties for Government employees who disclose cotton statistics, agricultural marketing agreements, Census information, certain information filed with the SEC, diplomatic codes, Civil Service examination information—that, indeed, carries a mandatory minimum sentence—crop information, trade secrets, bank and credit information, tax information, patent information classified for national security reasons, Social Security information. All of these Congress has said must be secret and has imposed criminal penalties on those who disclose.

As the wealth of information proliferates and the technology for collecting, storing, and transmitting it explodes, it becomes, as both previous witnesses have said, increasingly difficult to strike the proper balance between openness and free communication and necessary confidentiality.

This is reflected over our legal experience in the past decade. In the fall of 1974, Congress enacted the Privacy Act, to which Mr. Plesser referred, instructing the executive branch to collect less, protect it from public disclosure, reduce sharing among Government agencies and make less use of the Social Security number as an identifier.

In that same month, it passed legislation instructing the executive branch to make more information public and to use the Social Security number as an identifier so that information could be shared among agencies to identify and locate those who fail to meet child-support obligations.

In the following year, it enacted the Right to Financial Privacy Act, which originated in this subcommittee, to protect the confidentiality of banking records and an Ethics in Government Act which makes financial information of certain individuals totally public.

The Paperwork Reduction Act, like its predecessor, the Federal Reports Act, enjoins Federal agencies to share more information so the rights of individuals, particularly small businessmen, will not be infringed by having different Government agencies make the same inquiry again and again.

This illustrates the difficulty in trying to sort out what is or what is not properly protected, properly required, open, secret, and there are serious difficulties. The committee has looked into them in several areas and I won't go over all of them. They are each

but not control the speaker with the schematics in his head, we have done nothing to prohibit proliferation of nuclear weapons.

We don't have a solution, Mr. Chairman, I am simply raising it as a problem, but one that does have two sides, not merely one.

I had not planned to go into the Foreign Intelligence Surveillance Act since, as you noted, I had testified on that before this subcommittee, but I would mention in light of the comments made earlier, a couple of aspects of it.

The Foreign Intelligence Surveillance Act does not rely on the trespass concept that Mr. Shattuck referred to, the property concept of intrusion. It relies on the expectation of privacy concept recognized by the Supreme Court so that, unlike title III, which is, of course, an older statute, the expectation of privacy in the constitutional sense is the touchstone on whether or not a warrant is required under the Foreign Intelligence Surveillance Act.

That act defines electronic surveillance in much broader terms than does title III. It encompasses closed circuit television; it encompasses at least some forms of computer acquisition. It encompasses devices which track vehicles onto private property and it encompasses them not only in the sense of authorizing the Government to use those techniques with a warrant, but also in criminalizing persons who do so without a warrant. So to some extent, there is a criminal law now on the books, broader than the foreign intelligence field, which begins to address some of these concerns of the more recent technology, though not all. Clearly, it does not cover all of the difficulties.

Title III, as has been noted, relies exclusively on aural acquisition, that is, by ear, in both its criminal penalty and its warrant authorization. Consequently, many forms of electronics are not encompassed in title III.

As you noted earlier, Mr. Chairman, we do indeed believe that closed circuit television can be a legitimate form of electronic surveillance in criminal or foreign intelligence cases with a warrant. Our problem is that title III does not permit a warrant for that purpose because it is not aural acquisition and rule 41, with its requirement of notice and inventory, is simply not adaptable to that form of surveillance. So in the past we have asked courts to fashion a unique order in the nature of a search warrant with the same probable cause, but not with the same notice and inventory. That, however, has been called into question and has recently come under challenge in the courts, and this area of the law needs to be

The whole area of computers and privacy, as has already been stated and I won't go over that again, is an immensely complex one. We have introduced legislation to deal with one aspect of it and that is the intrusion into computers by individuals for the purpose of manipulating the computer, taking out information from a computer, destroying computer programs or, for that matter, destroying computers themselves and this legislation, criminal legislation, has been introduced. Again, it is unlikely to deal with all the problems, but it is a beginning in the area of computer fraud, in the area of computer destruction and malicious manipulation.

Finally, I think I had best address the issue of prepublication review. First of all, the order that was issued by the president, NSDD-84, does not and never has covered all individuals with access to classified information. It is limited to a narrow area of classified information. But the practice of prepublication review is one that is much older than that order and far broader within the Federal Government.

Early in my career, I was assigned the task of reviewing an article prepared by a Department attorney to ensure that it did not contain nonpublic information obtained through his Government employment. The regulation prohibiting that disclosure did not then, nor does it now require prepublication review. It does, however, like many of the statutes I listed before, impose a nondisclosure obligation on Federal employees, and the surest way to see that that obligation is met is to have the material reviewed in advance.

Department attorneys, indeed, all Government attorneys, have, in addition, the obligation to observe the grand jury's secrecy provisions of rule 6(e) and the attorney/client confidentiality prescribed by the Code of Professional Responsibility. In my own experience, the most effective way to meet these obligations is to get a second opinion, that is, submit an article for prepublication review.

I have submitted articles myself, none of them having to do with intelligence information and all of them predating NSDD-84, and I did so to fulfill my obligation as an attorney and to fulfill my obligation as a Department employee not to disclose inside information for my own benefit.

Much of the criticism of prepublication review has focused on it as a form of censorship, but I submit this is a slanted view. As I mentioned, Congress has imposed a number of nondisclosure obligations on Federal employees and it has done so presumably because they come into possession of information under a duty of public trust. Prepublication review is a prophylactic form of law

gress has attached on unauthorized disclosure and among the most severe penalties Congress has authorized are those dealing with unauthorized or even negligent disclosure of classified information. Presumably this reflects the judgment that the harm flowing from disclosure is great.

In imposing a prepublication review requirement beyond that traditionally imposed by CIA and NSA, NSDD-84 did not encompass the full range of information protected by the espionage laws. It singled out only those having access to the most sensitive categories of information.

Many of these are already covered by prior CIA and NSA review requirements. Others, like myself, share access to this information and, accordingly, are asked to share the same obligation. It is one I would have undertaken in any case.

The subcommittee may not be aware that former Attorney General Bell submitted to prepublication review in 1981, long before NSDD-84, those chapters of his book dealing with intelligence matters, not because of any signed agreement, but because of his appreciation of the sensitivity of the subject matter. As far as I know, his coauthor, a professional journalist, did not object to this.

That, I think, is where I will stop, Mr. Chairman, and we will go to questions.

[The statement of Ms. Lawton follows:]

STATEMENT OF MARY C. LAWTON, COUNSEL FOR INTELLIGENCE POLICY CONCERNING
1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE

Mr. Chairman and Members of the Subcommittee,

The topics you have asked us to address today are so diffuse that I would like to begin with some general observations on the concept of secrecy within an open society. While this might appear to be a paradox it is, in fact, a reflection of the essence of American society which from its inception has contemplated a balancing of values and individual rights.

This society has always recognized twin values of openness and confidentiality. The Constitutional convention that structured our government with its value of openness met in secret. All records of those meetings were sealed for more than thirty years and most of the Framers acknowledged that without secrecy no constitution of this kind could have been developed. United States v. Nixon, 418 U.S. 683, 705 n. 15. The Bill of Rights proposed by our first Congress reinforced the twin goals of openness and confidentiality. While the First Amendment with its guarantee of free press is often cited as the touchstone for openness, it also protects the right to hold certain matters in confidence. The free exercise clause, for example, protects the right to hold private religious beliefs not subject to scrutiny. Torcaso v. Watkins, 367 U.S. 488. The right of assembly may, in certain circumstances, include the right to protect the identity of one's associates in confidence. Bates v. Little Rock, 361 U.S. 516.

Neither our law nor our tradition has condemned secrecy or confidentiality as inherently wrong. Indeed, both have affirmed secrecy in its proper place as essential to our form of government. The secrecy of the Grand Jury has always been accepted as protection not only of the individual but of the legal process as well. Our rules of evidence recognize the importance of protecting certain confidential relationships: attorney-client; priest-penitent; physician-patient; and the State secrets privilege which protects both diplomatic and military information which must be held in confidence in the interest of national security.

Congress has singled out some types of information as so sensitive that those entrusted with it are subject to criminal penalties if they disclose it. This includes not only the sensitive national security information protected by the espionage and atomic energy acts but also such diverse information as: cotton statistics (7 U.S.C. 472); agricultural marketing agreements (7 U.S.C. 608e); census information (13 U.S.C. 214); certain information filed with the Securities and Exchange Commission (15 U.S.C. 78ff); diplomatic codes (18 U.S.C. 952); civil service examination information (18 U.S.C. 1917); crop information (18 U.S.C. 1902); trade secrets (18 U.S.C. 1905); bank and credit information (18 U.S.C. 1906-1909);

tax information (26 U.S.C. 7213); patent information classified for national security reasons (35 U.S.C. 186) and social security information (42 U.S.C. 1306).

As the wealth of information proliferates, however, and the technology for collecting, storing and transmitting it explodes, it becomes increasingly difficult to strike a proper balance between openness and free communication, on the one hand, and necessary confidentiality on the other. This is reflected in our legal experience over the past decade. In the fall of 1974 Congress enacted privacy legislation instructing the Executive Branch to collect less information, protect it from public disclosure, reduce its sharing among government agencies, and make less use of the social security number as an identifier. In the same month, it passed legislation instructing the Executive Branch to make more information public, and to use the social security number as an identifier so that information could be shared among agencies in order to identify and locate those who have failed to meet child support obligations. In the following years it enacted a Right to Financial Privacy Act to protect the confidentiality of banking records and an Ethics in Government Act which makes the financial information of certain individuals totally public. The Paperwork Reduction Act, like its predecessor, the Federal Reports Act, enjoins federal agencies

to share more information so that the rights of individuals, particularly small businessmen, will not be infringed by having different government agencies make the same inquiry again and again.

The casual observer might view these legislative "shifts" as "schizophrenic" but on closer scrutiny they merely reflect the twin values of openness and confidentiality and the difficulty in balancing these values in an increasingly complex world.

The hearings this Subcommittee has undertaken over the past year have focused on just a few of the areas in which the conflict is highlighted. I will comment on each of them briefly.

The press was not given advance notice of the Grenada mission and was not invited along. It protested vigorously and repeatedly cited the fact that it had been accommodated in all previous military actions throughout our history. While the historic argument is important and instructive, it does not address today's circumstance of news reports transmitted by satellite around the world in a matter of seconds. New technologies make new solutions important, particularly when one is

dealing with military actions in which the element of surprise is crucial. The Commission which was created following the Grenada action, involved both the press and the military in seeking these new solutions. Only time will tell whether their proposals have arrived at the proper balance.

The problem of scientific communication in an ever-shrinking world poses a more difficult issue. Academic freedom, while not mentioned in the First Amendment, clearly derives from its principle of the free flow of ideas. Yet the concept of protecting ideas from expropriation by others is a least as old as the patent and copyright clause of the Constitution. Art. I, sec. 8, cl. 8. In the modern world in which research in physics has translated into weapons of mass destruction and chemical and biological research can produce plagues far worse than those which decimated Europe in the Middle Ages, the free flow of scientific information can also mean the proliferation of weapons. How then do we square non-proliferation treaties and Export Administration Act controls with the free flow of information at international scientific gatherings and increasing exchange programs of students? It would be insane to train the scientist from abroad who is bent on developing the weapon that will destroy us and equally insane to deny training to the scientist who will develop the agricultural technology

necessary to feed the underdeveloped countries. It is pointless to embargo the latest prototype of a particular weapon if the scientist who has the schematics in his head can lecture freely on that subject to scientific gatherings that may include scientists from the embargoed country. We are faced here with the mirror image of the communications technology explosion. Our laws have developed the theoretical basis for banning the exportation of the very latest in communications technology, because it is tangible and fits within our traditional customs laws, but we have not yet found the solution to prevent the same exportation by the oldest form of communication, word of mouth. We are working with the scientific community, as Dr. Press has already noted, in attempting to strike the proper balance. We have no solution as yet. My only point in addressing the problem, Mr. Chairman, is to underscore that it is a legitimate issue. The question is not simply shall we have academic freedom? Rather it is a question of how to maintain both academic freedom and our national policy concerning non-proliferation and the control of U.S. technology.

I have already testified before this subcommittee on the subject of the Foreign Intelligence Surveillance Act and the procedures it establishes to strike a balance between national security and individual rights. I do not propose to repeat that

here. Rather, I would like to note some of the difficulties that have arisen under the criminal wiretap provisions which were passed in 1968. That law, in my judgment, strikes a proper balance between individual rights and law enforcement needs. It is, however, dated with respect to the new technologies which have developed in the last fifteen years. As has been pointed out by previous witnesses, new forms of digital communications, not to mention the capability of minaturized closed circuit television, have provided new forms of surveillance, some of great importance to law enforcement, which are not encompassed within Title III with its emphasis on "aural acquisition." Some of these involve an expectation of privacy which, under our Constitution, necessitates a warrant before law enforcement intrusion is permitted. Yet Title III makes no provision for such a warrant and Rule 41 of the Federal Rules of Criminal Procedure, in its literal terms, is not a satisfactory substitute. That rule, as you recall, requires immediate service of the warrant and receipts for items "seized." As Title III recognizes, this is not feasible in the surveillance context. In the past we have persuaded judges that there is inherent authority to use the delayed notice approach of Title III in crafting an order for closed circuit TV surveillance, even though Title III itself is not applicable. This has

recently been called into question, however. It may be a more systematized approach is needed, one that will survey all of the existing technological advances in light of the law enforcement and privacy interests to be advanced.

The issue of computers and privacy is even more complex and, in some ways, more emotional. While an increasing segment of society is becoming computer literate, there are still many within our population who are slightly awed and frightened by computers. Americans have always touted efficiency and speed as the best way to do business, the ideal way to provide services. Computers offer that efficiency and speed and, today, at less cost. Now many have begun to wonder whether the price paid in privacy loss by virtue of that efficiency and speed is not too great. When sheer inefficiency was our greatest privacy protection, we did not trouble greatly about other forms of privacy protection. In the mid-seventies, we concentrated on controlling what was entered into computers in order to protect privacy. Concern now is beginning to shift toward what is drawn out of computers and by whom. Hackers, often on a lark, are invading privacy just for fun. With or without malicious intent they also run the risk of altering or even erasing vital computer data. Manipulators have learned that they can steal

vast sums with slight computer changes. Industrial spies are concentrating on the theft of computer programs. Our laws concerning theft and malicious destruction of property are not drafted for the computer age. Our laws on privacy are largely directed against the government, not our fellow citizens. The Congress is now considering a bill developed by the Administration that we believe would resolve these difficulties and make such activities a crime.

Finally, Mr. Chairman, you have requested that we address the subject of pre-publication review. While this concept of reviewing written material of those who are under a non-disclosure obligation in advance of publication has drawn particular attention since the issuance of NSDD-84, the practice itself is much older and extends beyond the area of national security. Early in my career at the Department of Justice I was assigned the task of reviewing an article prepared by a Department attorney to insure that it did not contain nonpublic information obtained through his government employment. The regulation prohibiting such disclosure, 28 C.F.R. 45.735-12, did not then, nor does it now, explicitly require pre-publication review. It does, however, impose a non-disclosure obligation on all Department employees and the surest way to meet the

obligation is to have material reviewed in advance. In addition to this regulation, department attorneys have an obligation to insure that any writings or lectures they give do not breach the grand jury secrecy provisions of Rule 6(e) of the Federal Rules of Criminal Procedure or the attorney-client confidentiality prescribed by the Code of Professional Responsibility. In my own experience the most effective way to insure that I have met these obligations is to get a "second opinion," i.e., submit an article for prepublication review. I might add that the articles I have submitted pre-date NSDD-84 and had nothing whatever to do with intelligence information.

Much of the criticism of prepublication review has focused on it as a form of censorship. I submit that this is a slanted view. As I noted at the outset, Congress has imposed a number of non-disclosure obligations on federal employees enforced by criminal sanctions. It has done so, presumably, because they come into possession of the information under a duty of public trust. Pre-publication review is a prophylactic form of law enforcement to insure that the obligations of public trust are met. It is not the employee's ideas which are subject to review but rather the underlying government information. Of course, one could assert that the criminal sanction, imposed after

information is released, is sufficient enforcement. But this overlooks the damage that disclosure may cause to an individual's privacy or economic interests or to the broader interests of the nation.

The more sensitive information is and the more harm disclosure may cause, the greater the need for prophylactic measures. There are, of course, many yardsticks by which to measure harm potential. One such yardstick is the severity of the criminal penalties Congress has attached to unauthorized disclosures. Among the most severe penalties Congress has authorized are those dealing with unauthorized disclosures or even negligent disclosures of classified information. 18 U.S.C. 793-798. Presumably this reflects a judgment that the harm flowing from disclosure is great.

In imposing a prepublication review requirement, beyond that traditionally imposed by CIA and NSA, NSDD-84 did not encompass the full range of information protected by the espionage laws. It singled out only those having access to the most sensitive categories of information. Many of those covered are already covered by prior CIA and NSA review requirements. Others, like myself, share access to this information and, accordingly, are asked to share the same obligations. It is one which I would have undertaken, in any case, given the sensi-

vity of the information and the harm it could do my country. Nor am I alone in this view. The Subcommittee may not be aware that former Attorney General Bell submitted for pre-publication review in 1981 those chapters of his book dealing with intelligence matters, not because of any signed agreement but because of his appreciation of the sensitivity of the subject matter. Others have done the same. As a personal note, Mr. Chairman, I might add that whether or not Congress restricts the use of prepublication review agreements, I propose to continue to seek that "second opinion" before writing anything that may impinge on the national security.

I will be happy to answer any questions.

Mr. KASTENMEIER. Thank you, Ms. Lawton.

May I observe, however, merely because some people, including yourself and former Attorney General Bell, for various reasons submit to prepublication review even if not required to, that does not sanctify the procedure. There may be those who volunteer for military service. Merely because some volunteer for military service does not mean that others who may have objections to military service may not have a case to be made.

On the question of complaints that some scientists and acadami-cians have made that technology transfer has impinged upon their freedoms, why isn't classification sufficient? Why have we cracked down on scientists and others who feel they ought to be free to engage in exchange of scientific papers and the like?

Ms. Lawton.

Ms. LAWTON. Well, classification, of course, can only be imposed, under the current structure, on a thing, an object or a piece of paper. Where the spoken word is derived from such an object or a piece of paper, it remains classified as the paper or object was, but that which is yet to be reduced to a classifiable form may, nevertheless, be classifiable in its content.

Where you have Government contracts, that is one issue and the system is arranged for the Government to classify, but where you do not, the information may be such that would in the hands of the Government be classified, but there is no one out there to classify it in the academic setting. Now, there certainly is fundamental basic research as distinct from applied research that is probably so esoteric and so broad in its nature that there is no basis for classifying it or limiting its exportation or otherwise restricting it, but there are matters with which we are concerned. The export control laws, you will recall, put different rules as to different countries for the same information.

A computer, which is not classified in this country and not restricted in its export to some portions of the world is, nevertheless, by statute, restricted to export to other portions of the world. That is easy to do with a tangible object. They may ship it here, but not there. It is harder to do with the spoken word in a mass meeting where people from both here and there are present. That is the problem. That is why we have brought the academic community in to help us try to resolve it.

We have not issued the new regulations. We are working on them and we are working with the scientific community to try and resolve these issues.

Mr. KASTENMEIER. I understand you. The cases in court have indicated that universities and open scientific communication have been the source of very little of this so-called technology transfer problem. I am wondering whether we may not overreact in that regard and create a climate in this country that is adverse to the intellectual exchange of ideas. That would be a great price to pay for these fears.

Mr. Plessler, in suggesting that not much was being done in the administration with respect to some of these problems, were you not, in fact, indirectly or directly calling for the creation of some new entity for purposes of privacy or classification or whatever in terms of the problem as contemplated today?

Mr. PLESSER. Well, I think so. One of the important recommendations of the Privacy Commission, of which I was general counsel, was a permanent entity in the Federal Government that would study the issues, but also be—would go a step farther and give guidance to Government agencies in the implementation of the Privacy Act and related statutes. I see the need for that almost greater now than I did in 1977 and I do call for the establishment and think that it would be important to have an entity in the Federal Government.

I guess part of my hesitation in putting it forward is that it seems from, as a result of the GAO report and some of the other reports that we have seen, that the current administration, until this morning, I must say, because I think some of the things Mary said were really very positive in acknowledging and recognizing some of the concerns and the need to look at it, but really—but for what I have heard this morning, the reaction has seemed so negative in the administration—if not negative, almost just nonexistent, viewing it as a—with no interest in it and as a nonissue, that it is a little—I feel a little uncomfortable in recommending a permanent entity to be established and manned by people who really seem to have no interest in it.

But if there is some interest and concern in it, I think that there really does need to be an entity on the Federal level looking at it along the lines that the Privacy Commission recommended, and as I said before, it was that kind of entity, I think, that was also recommended by the ABA panel that met this summer.

Mr. KASTENMEIER. As was recognized by the GAO report on privacy activities, NTIA funding for privacy personnel had dropped from 15 positions in 1979 to 6 in 1981 to 1 current position. That would suggest that privacy protection is diminishing.

Mr. PLESSER. I think it is viewed as a nonissue. I hate to say that it is even a negative reaction because it is almost like a marshmallow. There is no reaction. It is simply, you know, other than in obviously in the Justice Department takes positions on warrants and access to information, but if you get beyond that into what NTIA has been doing, there really just is no response.

I spent some time in Europe this last spring meeting with international privacy people and there is really great wonderment over there that there is so little demonstrated concern on these issues in this country. I don't really know what the basis of it is because I am not sure the privacy is really a political issue one way or the other. It is just simply an issue that is going to become more and more acute with the advancement of technology. I thought Ms. Lawton's comments this morning on the cordless telephone were correct. Unfortunately, the Supreme Court of Kansas disagrees with both of us, and the Supreme Court of Kansas is writing the rules so far and the Supreme Court of Kansas has said that there is no expectation of privacy for conversations on the cordless telephone and one of the facts of that case is that at some point the police were listening directly to the FM radio. It wasn't just given to them by private sector—by private individuals, and the really shocking part of that decision is the Supreme Court of Kansas said there is one issue here that we haven't resolved and we will put off until a later case and that is what is the expectation of privacy of the person on the other end of the line who has no idea of the technology being used. Whether or not it is a cordless phone or a regular phone, the person on the other end of the phone is expecting that it is a private communication protected by title III. But the Supreme Court of Kansas says, no, it is not protected by title III because it is interceptable by a radio-telephone. That kind of issue needs to be resolved and discussed, not only by the courts, not only by Congress, but also by the executive branch. I have seen almost nothing from the executive branch and I believe that an entity does need to be developed. Even if I disagree with what they come out with, at least it becomes a target and it becomes a debate so that we can go forward.

Mr. KASTENMEIER. One last question on that. Are you talking about an entity that is advisory? Does it have enforcement powers? Is it another commission?

Mr. PLESSER. I don't think it should be another commission in terms of temporary. I think it should be advisory in study. I think some of the things that NTIA had done should be done by such an entity, but I also think it should take over some of the guideline roles that OMB has had in privacy enforcement. I think it should be in a position of issuing binding rules and guidance for the Government agencies in terms of how they operate under these laws.

Mr. KASTENMEIER. Ms. Lawton, as Mr. Plessler noted, you discussed the differences as you see them between title III and its limitations and FISA and its broader coverage. I suppose what has happened is it leaves people in the position of assuming either certain things in the middle are clearly covered or they are not covered and no warrant is required or they are not covered and are forbidden.

Presumably there could be activities on either side of the line for which someone presumes authority without a warrant, or they could try to get a warrant with some form of implied authority on the part of the court, or they could presume that the activity was, in fact, unauthorized by statute and illegal.

That does leave an unsatisfactory state of the law. In title III, it is even worse since the word "aural" communication is so explicit.

Why hasn't the administration recommended to us some statutory language to improve either or both of those old laws? They are outdated.

Ms. LAWTON. It is a question of one thing at a time, I think, primarily, Mr. Chairman. The big concern—well, the FISA penalty, as I said, does cover some things that title III does not. It is, after all, only applicable to those who act under color of law. People only seem to be worried about government invasions of privacy, not anybody else's. Title III, of course, covers anybody who wiretaps, but only that which is the aural communication.

We had, in recent years, a couple of examples of serious computer crimes, both in terms of people stealing from computers by manipulation of programs and then the highly publicized hacker incidents, including the penetration of a medical computer at Sloan-Kettering, which really worried people. So, the first thing we took a look at was trying to come up with legislation to deal with that problem and that is the legislation we have proposed because there was nothing to cover that situation, not even by argument or extension of existing legislation.

So we thought to plug the gap first. That is not to say that we will not take a look at title III; it is just a question of being able to deal with one thing at a time, as we approach this area which is very difficult because, at least in Justice, it is the lawyers who draft the legislation and they are not too swift on the technology of the whole thing.

Mr. KASTENMEIER. It is my understanding that the administration's approach to computers, computer privacy, and computer crime or fraud is narrower than that of the bill that was processed by the Congress. Unrestricted access by individuals, private companies, and Government agencies is not really included in the computer crime bill recommended by the administration, while I think the committee bill does include that.

Ms. LAWTON. Well, one of our concerns, and one of the reactions we got was on the whole question of jurisdiction. There is always the federalism problem. By what authority does the Congress occupy a field of criminal law enforcement that could be occupied by States? So we drafted the statute with specific Federal interest as the base for the Federal jurisdiction.

That is, Government computers, federally insured financial institutions and interstate communication, just as the current wire fraud statute requires an interstate nexus and does not cover any use of the telephone. That is basically the reason why the other bill, as I recall, does not—refers generally to affecting interstate commerce, but without as tight a definition of what that means.

Mr. KASTENMEIER. Mr. Plessler, did you—

Mr. PLESSER. I would just like to make one comment which is, I was at a hearing of the Senate Judiciary Committee 2 weeks ago

where a colleague of Ms. Lawton's from the Justice Department testified on whether or not title III should be amended to solve the aural problem and it was my recollection at that point that there was not a question of not getting to it; it was a very affirmative position that the law should not be changed. The Justice Department saw it as an unwarranted and unnecessary action that could affect their ability to obtain information. So while I appreciate Ms. Lawton's comments this morning, I think it should be noted on the record that officials of the Justice Department are not all in agreement on this issue.

Mr. KASTENMEIER. Mr. Shattuck, in your own testimony on national security issues, you referred to another point in time that started in the Nixon years, as I recall.

The fact is, apparently, that whatever threat there is to national security remains a rather constant one. Granted, we have an adversarial relationship with the Soviet Union or socialist countries in the political and the ideological and military fields, among others. I take it that historically, though, this has remained constant—a more or less static situation.

Yet, we have had ups and downs in terms of how this Government has responded to the perceived threats. You referred to an era under Mr. Nixon. All three branches of our Government responded to that by making a number of changes in the 1970's under Presidents Ford and Carter and Attorneys General Levy and Bell and then things apparently started to heat up again until we have the current situation. You cited a number of things that suggest that we are entering into a new era. I don't know whether it is as pernicious in that respect as the Nixon years you referred to.

I don't think this is necessarily a Republican versus Democratic question. I wonder what your analysis is, why we have these ups and downs and irregularity in terms of response to a threat that is presumably fairly stable.

Mr. SHATTUCK. Well, that is the big question and I think it is certainly true that while the threat, as you have defined it, is relatively constant, it is perceived differently from time to time and I think it is addressed differently from time to time.

I would like to answer the question by being quite specific in terms of the issue of export controls and the growing difficulties that Ms. Lawton was referring to of trying to define how national security can best be protected in the context of scientific research and the technological information that comes out of that research and that will find its way overseas.

Until quite recently, it was generally assumed that scientific research on campus—basic research was referred to before, or sometimes even applied research—would not produce information which would then fall within the confines of the export control system. What we have today, I think, is a sense that somehow national security can best be protected by clamping down on certain kinds of scientific information which is inherently dangerous, which, if falling into the wrong hands, would come to harm us. Yet, as many experts in this field say, that is often a counterproductive way to protect national security. Edward Teller, who was not otherwise noted for his strong civil liberties views on a range of matters, is perhaps the best witness on this point. He thinks that the applica-

tion of export control systems to a growing field of scientific information is very damaging to the national security because it will reduce the innovation that is necessary in order to have the United States remain strong in certain basic scientific fields, strong not only in terms of basic research, but also in terms of applied research and in terms of—in his view—the development of certain weaponry that would come out of that research.

So I think what we have is, in answer to your question, a changing climate in which it is regarded as acceptable to assert certain kinds of controls on the free flow of information, not only acceptable, but necessary, because it will protect us against the disclosure of that information in the world at large and yet, there is a very different point of view which prevailed not terribly long ago and that is that the great strength and national security of this country is, in fact, the free flow of information and ideas, even if there is a risk that some information may, in fact, be dangerous.

If it is genuinely dangerous and in the control of the Government, then it can be subject to the Government's information control systems known as the classification scheme, but if it is out there in the world and it is being produced in the context of scientific research to say that it is either "born classified" or, as the new Executive order on classification in effect says: "It can become classified over time," is to provide a very different and much broader kind of control system.

I think that what we have seen in this area of information controls is an illustration of the changed perception of what national security requires—changed today over not terribly long ago and changed very much for the worst, not just from the point of view of civil liberties, but from the point of view of genuine national security, innovation, competition, development of resources and remaining strong in the world.

There are others in private industry who take very much the same point of view with respect to export controls.

Mr. KASTENMEIER. Thank you.

Ms. Lawton, Mr. Plessner, do you have any comments on that?

Ms. LAWTON. No, Mr. Chairman.

Mr. KASTENMEIER. I would like to ask Ms. Lawton one thing. I think you have correctly suggested that it isn't just the executive branch, but the Congress itself that was responsible for a lot of secrecy of classified information and you cited quite a few laws in that regard; but I know, too, that you are well aware that there has been criticism about overclassification, whether these are cotton statistics or Defense Department material or whatever. There is a tendency on the part of anyone, for whatever purpose, to overclassify and to make information inaccessible.

Is there anything we can do about that in your view? Would you concede that, we may be as bureaucrats, overclassifying material?

Ms. LAWTON. Certainly there is overclassification. There is now, from my own perspective and indeed from the studies done by the Information Security Oversight Office considerably less overclassification than when I came to Government, much less. I think that is for a variety of reasons. One is that the last three Executive orders on the subject have required paragraph-by-paragraph classification. Not everybody complies with that, but it is required and that

makes you think about, not the subject matter of the memo, but the content of a paragraph. When you have to think about that, there is less classification you have to justify each paragraph. That, I think, has reduced it.

There is an Information Security Oversight Office that comes in and audits agencies and checks on whether they are properly classifying or not. That is relatively recent. I think the system has improved considerably. Certainly it can be improved more and there are areas of overclassification, but in my own personal experience over 24 years of Government, there is much less overclassification now than there used to be.

Mr. SHATTUCK. Mr. Chairman, can I make a comment on that point?

Mr. KASTENMEIER. Mr. Shattuck.

Mr. SHATTUCK. I think the perspective that has just been stated has to do with what the behavior of those who are engaged in classifying may be. The fact of the matter is, however, that the new Executive order on classification is, the broadest ever—it gives the broadest authority and the greatest amount of discretion. In fact, in some cases, it is not even discretion; it is essentially a mandate to classify. In a number of key areas it is broader than anything we have seen before.

I would just mention four specific ways in which it is substantially revised over the earlier Executive orders. First of all, it eliminates any kind of balancing test, which would require those engaged in the classification process to think about whether there is public interest in the disclosure of certain information and weigh that against the Government interest in maintaining its secrecy. Second of all, there is a shift in the presumption which existed in the earlier Executive order which is essentially when in doubt, don't classify, to, under the current order, when in doubt, do classify, and when in doubt as to what level of classification to apply, apply the higher level as opposed to the lower level.

Third, it provides new authority to reclassify and classify information that may already be public, as I was referring to before, which is a matter of considerable concern on campus in that people may make a decision to enter into certain kinds of technical research areas and then find out somewhere down the road that the information that is being produced in that area may be falling into some general classification scheme.

Fourth, it eliminates the standard for classification of some identifiable damage to the national security so that the new standard, does not require a classifier to identify any particular kind of damage or any damage that might be identified before the decision is made to classify. So in at least four major ways, and many others that are set forth in the report that I have provided to you, this new classification order is the broadest that we have seen in the entire post-World War II era since the classification system went into effect.

Mr. KASTENMEIER. Is there any way of knowing quantitatively how much we have or whether it is more or less than we had 5 or 10 or 15 years ago?

Ms. LAWTON. The Information Security Oversight Office makes an annual report to the President, which is also furnished to the

Congress, and I think it does some comparison. I don't know how many years back it goes, but I think it certainly talks about numbers of persons with authority to classify and I believe it also talks about documents and also the numbers of surveys and audits that have been done in terms of going in and checking on the practices of individual Government offices.

So there is some of that there, Mr. Chairman. I don't know how far back it goes.

Mr. KASTENMEIER. What role has Congress had in this? Could it have imposed more stringent standards on the executive branch so as to ensure that that which is classified is only that which should be classified?

Mr. Plessner, do you happen to know?

Mr. PLESSER. There are some constitutional prerogatives and some traditions that Congress may not be able to affect. Congress has put out some mixed signals on this, I think that we can go through most of those examples and say that there are perhaps competing interests and no one is suggesting that there has to be complete openness on all information. I don't think there is really much conflict between export controls on one hand and on the other hand, a desire for open information in terms of Pentagon or Defense Department contracting.

I think they are just two totally separate issues. Export controls are for economic reasons, as well as for security interests. It is very difficult in export control to determine when restrictions are being made for security or economic reasons. Most controls are to control the availability of rare materials or precision tooling—that is really not a question of information; it is just that we do it better and we don't want those products going to other people. You can have export administration controls to preserve domestic markets.

On the question of classification, the Executive order now is as broad as any we have had to deal with, but I also probably agree that a great deal of information is now being released.

Mr. KASTENMEIER. Thank you.

I would like to go on to one other thing. The Justice Department has issued guidelines for video surveillance, Mr. Plessner. Under what circumstances do you think that such surveillance may be justified? What are the dangers of it? What might be the safeguards?

Mr. PLESSER. I am not completely familiar with those, but I think that the real danger is in the mixed technologies. I mean they are the real concerns that I have. When something is part radio, part cable, part wire, it is simply impossible for us to know when we make a transaction on a telephone on what technology it is going to be carried.

If I make a phone call to New York, it may be on a wire; it may be on a microwave; it may be on a satellite transmission. I have no way of knowing how that communication is going to be done. Certainly if I am on the receiving end of a telephone from a cordless telephone as well, I don't know.

I am not familiar enough, I think, with the regulations, though, to comment on them. Maybe Ms. Lawton would comment on them more directly.

Mr. KASTENMEIER. Ms. Lawton, would you like to comment on the guidelines for video surveillance?

Ms. LAWTON. I don't have them with me in terms of going into them in detail, Mr. Chairman, but first of all, of course, we are talking about—when you say "video surveillance," I am assuming you are limiting this now to the context of collecting evidence. We use video surveillance as a security technique rather commonly, but that is generally with a notice published and people are forewarned. For example in this store there are video cameras. We use it as we would use any other form of search in order to gather evidence.

It is particularly useful in those kinds of crimes where a transaction can be completed without words; a transfer of goods in a wink; the assembly of pipe bombs with the traditional wiretap producing only such evidence as: "Hand me the screwdriver;" "Give me that;" "Do you want some of this?" Nothing could be used in evidence. Combined with a video camera that shows that the screwdriver is to loosen the cap in order to get the detonator connected with the pipe bomb gives you a different form of evidence, much more useful in the courtroom.

That is essentially what we use it for. We use it with warrants.

Mr. KASTENMEIER. Yes; you have really two potential uses for video cameras: general surveillance, and then also for evidentiary purposes. I am reading from the Department of Justice directive:

Requests may be approved as a matter of course by one of these officials when no intrusion on the person's legitimate privacy rights appears to be involved. The most common situation is when a consenting party to the presence of the camera will be present at all times.

These are used, apparently, to record the scams and other things. It was pointed out that these surveillances are done in black and white to make them have a documentary type of appearance. They are persuasive in terms of viewing, at least to the public later on.

Ms. Lawton, you state on page 7 that title III does not apply to video surveillance, but that you believe there is an inherent authority to use it. You said also that this point is being litigated. Could you expand upon that?

Ms. LAWTON. Yes; Mr. Chairman, I will try to word this carefully because it is in litigation. In a criminal case in Chicago involving members of the FALN—and I can't remember what the Spanish letters stand for—the Government sought to introduce or proposed to introduce into evidence not only the electronic surveillance which was conducted on what the Government alleges to be a safe house, but also video surveillance of the same premises showing certain conduct which we allege to be criminal by the defendants.

The defendants filed a motion to suppress, challenging both the electronic—that is, the aural intercept, and the video intercept. The trial judge ruled the aural intercept admissible and the video intercept inadmissible and that is now on appeal to the seventh circuit.

We had a court order to do both. The problem is that the court order for the aural surveillance was clearly authorized by title III. We rely on rule 41 to get the video court order, but with a twist that says to the court, use the rule 41 authority to issue the court

order, but the title III type procedures for implementing it, rather than the rule 41 procedures. That is where we are now.

Mr. KASTENMEIER. Would the administration concede, Ms. Lawton, that we need legislation on the subject and we ought to clarify what the statute says?

Ms. LAWTON. I can't say what the administration would concede, Mr. Chairman, I haven't checked it out. Those of us who deal with the statutes are concerned that we need clarification, yes.

Mr. KASTENMEIER. Well, I am being called to the floor, so I think we will conclude these hearings. I want to thank all three of you, Ms. Lawton, representing the Justice Department; Mr. Plesser and Mr. Shattuck. It is always a pleasure to greet Mr. Shattuck, particularly back here in this capacity, although he speaks as an individual here this morning.

All of you have contributed in responding to some of the major questions with respect to civil liberties, to privacy, and to questions which the "1984" hearing series has addressed itself.

While this is the last hearing in the series, I doubt whether the questions on this subject end here today. Nonetheless, as a first step in contemplating the problems and possibly some of the solutions, I think this has been very useful.

I thank the three of you. I regret that more members of the Congress couldn't be present, but in any event, I will assume their interest in this subject is a continuing one.

Accordingly, the hearing is adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned, to reconvene subject to the call of the Chair.]

APPENDIXES

APPENDIX 1

APPENDIXES TO HEARING HELD NOVEMBER 2, 1983

APPENDIX I.—MISCELLANEOUS ARTICLES

- Cronkite, "Orwell's '1984'—Nearing?," *New York Times*, June 5, 1983.
 Abrams, "The New Effort to Control Information," *N.Y. Times Magazine*, Sept. 25, 1983.
 Shattuck, "National Security a Decade After Watergate," *Democracy* (Winter, 1983).
 Emerson, "The State of the First Amendment as We Enter '1984,'" *Yale L. Rep.* 15 (Spring, 1984).

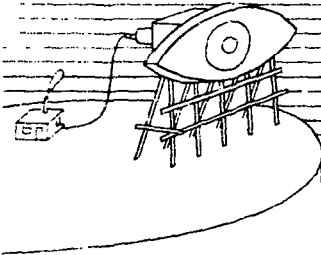
APPENDIX II.—MATERIALS RELATING TO RESTRICTIONS ON THE PRESS IN GRENADA

- H. Res. 384, 98th Cong., 1st Sess. (1983).
 News Release by the Secretary of Defense dated August 23, 1984, and attached Final Report of the CJCS Media-Military Relations Panel (Sidle Panel).
 Humphries, "Two Routes to the Wrong Destination: Public Affairs in the South Atlantic War," 36 *Naval War C. Rev.* 57 (No. 3) (1983).
 Gottschalk, "Consistent with Security" . . . A History of American Military Press Censorship," 5 *Comm. and the Law* 35 (1983).
 "U.S. Troops Remove Four Reporters," *Washington Post*, October 27, 1983.
 "Invasion Secrecy Creating a Furor: Speakes Complained in Memo," *Washington Post*, October 27, 1983.
 "Administration Limits News of Grenada," *Washington Post*, October 27, 1983.
 "U.S. Forces Thwart Journalists' Reports," *Washington Post*, October 28, 1983.
 "Censoring the Invasion," *Washington Post*, October 28, 1983.
 McCloskey, "Invasion and Evasion," *Washington Post*, October 28, 1983.
 "U.S. 'News Control' on Grenada?," *Washington Post*, October 28, 1983.
 "In Barbados, a Restless Press," *Washington Post*, October 29, 1983.
 "Information Out of Sync," *Washington Post*, October 29, 1983.
 Lewis, "What Was He Hiding?," *New York Times*, October 31, 1983.

- "Admiral Fights 2 Battles: With Grenada and Press," Washington Post, October 31, 1983.
- Grunwald, "Trying to Censor Reality," Time, November 7, 1983.
- "U.S. Press Curbs in Grenada May Affect International Debate," New York Times, November 8, 1983.
- Cockburn, "The Press and the Invasion," The Village Voice, November 8, 1983.
- Cohen, "Hey!," Washington Post, November 13, 1983.
- "Information Blackout Revives Old Issues," Washington Post, November 15, 1983.
- Cartoon by Herblock, Washington Post, November 16, 1983.
- "Shultz Defends Press Ban," Washington Post, December 16, 1983.
- Johnson, "Echoes," Washington Post, January 29, 1984 (Results of Harris Poll on the press in Grenada).
- Middleton, "Barring Reporters From the Battlefield," N.Y. Times Magazine, Feb. 5, 1984.
- "U.S. Bars Reporters From Naval Exercises," Washington Post, May 6, 1984.
- "Pentagon Plans Media Pool to Cover Missions," Washington Post, August 24, 1984.
- "Pentagon Forms War Press Pool; Newspaper Reporters Excluded," New York Times, October 11, 1984.
- Letter to House Committee on the Judiciary from Thomas J. Roche, Jr., dated November 4, 1983.
- Letter to Hon. Robert W. Kastenmeier from John Hendry dated October 30, 1983.
- Letter to Hon. Robert W. Kastenmeier from Ralph D. Bradway dated November 8, 1983.
- Letter to Hon. Robert W. Kastenmeier from Elbert N. Mullis, Jr., dated November 4, 1983.
- Letter to David Brinkley from S. H. Byers, President, Byco, Inc., dated November 4, 1983.

APPENDIX III.—PREPUBLICATION REVIEW PRACTICES BY GOVERNMENT AGENCIES

- Bamford, "How I Got the N.S.A. Files: How Reagan Tried to Get Them Back," Nation, November 6, 1982.
- Memorandum from William French Smith, Attorney General, to Heads of Offices, Boards, Divisions and Bureaus, dated March 11, 1983, regarding Presidential Directive on Safeguarding National Security Information.
- Burnham, "The Silent Power of the N.S.A.," N.Y. Times Magazine, March 27, 1983.
- Letter to Hon. Glenn English from Lincoln D. Faurer, Director, N.S.A., dated June 14, 1983. Attachment: Responses to Questions from Rep. Glenn English.
- Letter to Hon. Robert W. Kastenmeier from Don Sellar, Prairie Correspondent, Southam News of Canada, dated October 28, 1983. Attachments: "FBI Quizzes Canadian Correspondent About Source of Defense Information," the Washington Post, September 1, 1983. Arvidson, "The FBI Bears Down," Columbia Journalism Review, September/October 1983.
- Taubman, "Security Agency Bars Access to Nonsecret Material, Library Records Show," New York Times, April 28, 1984.
- R. McGehee, Deadly Deceits 196-203 (Appendix: This Book and the Secrecy Agreement).



Orwell's '1984' — Nearing?

By Walter Cronkite

In 1948, George Orwell wrote a novel satirizing the dehumanizing trends of the age. He first thought of calling it "The Last Man in Europe" but settled on a shorter title, transposing the last two digits of the date and giving the world a new synonym for tyranny: "Nineteen Eighty-Four."

How close have we come to his dark vision? Clearly, we aren't there yet. For one thing, 1984 will be an election year in America. In the world of Big Brother and the Thought Police, there were no elections anywhere. Still, if Winston Smith, the hero, were set down in today's world, there would be things he might recognize, along with some new threats to freedom his creator could not have imagined.

In the book, war and the excuse it provided for tight controls constituted a mechanism used by those in power to perpetuate their power. Orwell drew upon Stalinist Russia and Hitler's Germany for his inspiration, but it was the West that concerned him. He feared the impact of the cold war on the democracies' traditions, the ideologies of the left and right for whom ends justified means, the uses to which new technologies would be put.

An elite of ideologues, bureaucrats and scientists ruled a barely literate majority called the proles in Orwellian society. Would Smith recognize the origins of his world in a democracy such as ours, where technological complexity is on the rise and educational performance on the decline; where the result is a growing number of functional illiterates, barely able to cope in their personal

Walter Cronkite is a special correspondent for CBS News.

lives and clearly unfit to consider competently the affairs of the nation?

The State, or the Party, was the source of all information (and disinformation). Events were reported, or not, to fit the needs of policy; the past was rewritten to fit the current party line. Could Smith see the seeds of his Oceania in our society, in which the Federal Government tries to shroud more and more of its activities with "security" classifications; in which scientists keep the Government informed about their research; in which some of their ideas are stamped "classified" at birth?

Language, in the novel, was a primary tool of manipulation, and doublethink was a mental trick that had to be mastered by rulers and ruled alike. Doublethink was "the power of holding two contradictory beliefs in one's mind simultaneously and accepting both of them," of using "conscious deception while maintaining the firmness of purpose that goes with complete honesty."

In our world, where a Vietnam village can be destroyed so it can be saved; where the President names the latest thing in nuclear missiles the "Peacekeeper" — in such a world, can the Orwellian vision be very far away?

No image in modern fiction has so burned itself into public consciousness as Big Brother's eyes and the omnipresent telescreen. The total absence of privacy, the idea that the government is (or may be) always watching, means, most of us would agree, the ultimate loss of freedom. The two-way telescreen may have been a fantastic idea in 1948; the technology is here for 1984.

Our concern for security has led to an enormous growth in surveillance. There are cameras in banks, super-

markets and department stores; cameras watch hallways and alleys and entrances to buildings. In Miami Beach, there are cameras on street corners, monitoring the sidewalks.

Computers provide surveillance of another kind, gathering information on our financial affairs, buying habits, travel patterns. If we have cable TV systems at home, they may collect data on our viewing patterns. If we participate in a cable talk-back system, we may be giving a data bank our political opinions, with our names and addresses attached.

The Government, of course, already collects enormous amounts of information in data banks belonging to the Internal Revenue Service, Social Security Administration, the Census Bureau and a dozen or so other computers. If Big Brother could just get all the major private and government data banks in America linked, he might be 80 percent of the way home.

Big Brother's ears have plugs in them right now (or they are, by law, supposed to), at least on the side turned toward domestic telephone and cable traffic. But the National Security Agency's ability to monitor microwave transmissions, to scoop out of the air vast numbers of communications, including telephone conversations, store them in computers, play them back later, has a truly frightening potential for abuse.

George Orwell issued a warning. He told us that freedom is too much taken for granted, that it needs to be carefully watched and protected. He did not say his fictional vision of 1984 was bound to happen. He said it could happen — here. His last word on the subject was a plea to his readers: "Don't let it happen. It depends on you."

Maris Bischof

**INTENTIONAL
BLANK**

THE NEW EFFORT TO CONTROL INFORMATION

WE ARE,
a noted
lawyer
contends,
embarked on
a course
that seems at
odds with
the basic
tenet of
the First
Amendment.

By Floyd Abrams

A MONTH AGO TODAY, THE REAGAN ADMINISTRATION publicly released a contract that has no precedent in our nation's history. To be signed by all Government officials with access to high-level classified information, it will require these officials, for the rest of their lives, to submit for governmental review newspaper articles or books they write for the general reading public.

The contract will affect thousands of senior officials in the Departments of State and Defense, members of the National Security Council staff, senior White House officials and senior military and Foreign Service officers. Its purpose is to prevent unauthorized disclosure of classified information, but its effects are likely to go far beyond that. It will give those in power a new and powerful weapon to delay or even suppress criticism by those most knowledgeable to voice it. The new requirement, warns the American Society of Newspaper Editors, is "peacetime censorship of a scope unparalleled in this country since the adoption of the Bill of Rights in 1791."

The subject of hearings earlier this month of a subcommittee of the Senate Governmental Affairs Committee, this latest attempt at information control by the Reagan Administration is part of a far more sweeping policy. It is one unique in recent history — clear, coherent and, unlike that of some recent Administrations, not a bit schizophrenic. More important, it seems at odds with the concept that widespread dissemination of information from diverse sources furthers the public interest. In fact, it appears to be hostile to the basic tenet of the First Amendment that a democracy requires an informed citizenry to argue and shape policy.

In the two and a half years it has been in power, the Reagan Administration has:

- Consistently sought to limit the Freedom of Information Act (F.O.I.A.).
- Barred the entry into the country of human speakers, including Hortensia Allende, widow of Chilean President Salvador Allende, because of concern about what they might say.
- Inhibited the flow of films into or out of our borders; neither Canada's Academy Award-winning "If You Love This Planet" nor the acclaimed ABC documentary about toxic waste, "The Killing Ground," escaped Administration disapproval.
- Rewritten the classification system to assure that more rather than less information will be classified.

“THE EFFECT OF the new guidelines is to permit the Government itself to decide what information about its conduct is “meaningful.”

who wished to attend the session, his response was: “We have absolutely no legal obligation to let Tommy Bulgaria or anyone else from Soviet-front groups” enter the country.

Motion pictures have not escaped Administration scrutiny. Since its adoption in 1938, the Foreign Agents Registration Act has required any film that is produced under the auspices of a foreign country and that is political propaganda to be so labeled unless the film is “not serving predominantly a foreign interest.”

In the single most expansive, and best known, interpretation of the statute by any Administration, the Department of Justice last year sought to require three films produced by the National Film Board of Canada to be labeled as political propaganda. One of the films, “If You Love This Planet,” subsequently won an Academy Award. The Department of Justice later summarized the film’s “political propaganda” message this way: “Unless we shake off our indifference and work to prevent nuclear war, we stand a slim chance of surviving the 20th century.”

Why a film with such a message was considered political propaganda has yet to be satisfactorily explained. Why it was considered to be serving “predominantly a foreign interest” also remains unexplained. On May 23, 1983, Judge Raul A. Ramirez of the United States District Court for the Eastern District of California entered a preliminary injunction restraining the Justice Department from requiring registration of the three films.

“The court,” concluded Judge Ramirez, “is having great difficulty in ascertaining how any legitimate Federal interest is espoused or advanced by the classification of documents and/or films such as those before the court as propaganda. It makes no common sense whatsoever when we are dealing in a realm where the entire purpose is the dissemination of free ideas throughout the citizenry of the United States, so that citizens can bounce ideas off of each other to ascertain the truth.”

American-made documentary films destined for foreign audiences have not escaped scrutiny either. Under an agreement adopted by a United Nations conference in 1948, film makers pay no American export or foreign-import duties if the United States Information Agency (U.S.I.A.) certifies that they are primarily intended to “instruct or inform” rather than to propagandize.

It is the U.S.I.A. that decides on which side of the line — “information” or “propaganda” — a film falls. It, in turn, relies on the Government agency with expertise in the area to advise it. Under this Administration, as revealed in the July-August issue of American Film magazine, the result has been that the acclaimed 1979 ABC documentary about toxic waste, “The Killing Ground,” was denied a certificate. The Environmental Protection Agency (E.P.A.) concluded last year that the film was “mainly of historical interest” since the United States “has made great progress in managing hazardous wastes.” “The Killing Ground” had won two Emmys, first prize at the Monte Carlo Film Festival and been nominated for an Academy Award. Cut to its E.P.A. reviewers, “the tone of ‘The Killing Ground’ would mislead a foreign audience into believing that the American public needed arousing to the dangers of hazardous wastes [when] this is no longer the case.”

So intently has the Administration focused on the perils of disclosure of information that it has sometimes failed to distinguish between information previously made public and that which has been kept secret. When the unaccompanied luggage of William Worthy Jr., an American journalist, and his two colleagues arrived from Teheran at Boston’s Logan International Airport in December 1981, it included 11



Frank Snepp Jr., whose book, “Decent Interval” ran afoul of the C.I.A.

volumes of American Embassy documents said to have been seized by Iranians during the takeover of the embassy, reproduced by them and sold freely on the streets of Teheran. The documents had been secret. By the time the three Americans obtained a copy, they could hardly have been so to any intelligence agency in the world.

Nevertheless, the volumes were impounded by the F.B.I. and Customs officials at the airport. A year later, after the journalists had sued the Government, the two agencies agreed to an out-of-court settlement of \$16,000.

OF ALL THE POLICY CHANGES OF THE Reagan Administration from that of its predecessors, the ones that may have the most lasting impact are the decisions to classify more information and to subject Government officials to lifetime prepublication review.

This occurred in three stages, the first taking place eight months after the inauguration of the new President. One of Attorney General William

French Smith’s first major acts in 1981 was to revoke Justice Department guidelines issued just a year before concerning the United States Supreme Court decision in *Snepp v. United States*. In 1980, the Justices had upheld, by a 6-3 vote, a C.I.A. requirement that its employees agree to lifetime prepublication review by the agency of their writings to insure that no classified material was revealed. The Supreme Court concluded that someone subject to such an agreement who failed to submit his writings, even of unclassified information, breached the agreement. Frank Snepp Jr., a former C.I.A. analyst of North Vietnamese political affairs, was obliged to turn over to the Government all of his earnings from his book “Decent Interval.”

The Supreme Court ruling contained broad language that could be

**'THE ACROSS-THE-
board rejection of
the values of
information is
unprecedented. So
is the ease with
which those values
have been overcome.'**

interpreted to permit the same prepublication review procedure to be applied, as well, to the tens of thousands of non-C.I.A. employees who also have access to classified information. The Government had not sought that degree of power in the Snepp case. Nor is it clear that the Court intended that result.

Aware that in hands insensitive to First Amendment rights the Snepp opinion might be overextended, Attorney General Benjamin R. Civiletti issued a set of guidelines. They called for the Government to consider several alternative actions before rushing to Court to obtain injunctions against publication of unintentional and possibly meaningless disclosures of information. Among the factors to be weighed was whether the information already had been made widely available to the public and whether it had been properly classified in the first place.

In revoking the Civiletti guidelines, Attorney General Smith explained that his department sought to avoid "any confusion as to whether the United States will evenhandedly and strenuously pursue any violations of confidentiality obligations." However, no example was offered of any harm actually or even potentially caused by the Civiletti guidelines.

The second step taken by the Administration related to the classification system itself. The system had long been criticized for its absurd overinclusiveness. Between 1945 and 1963 alone, more than 500 million pages of documents had been classified. By 1973, 100 million pages of classified World War II documents still had not even been reviewed to determine if they should be made public. President Richard M. Nixon once observed that even the White House menu was classified.

A 1978 Executive Order signed by President Jimmy Carter attempted to limit the amount of information unnecessarily kept from the public. Government officials were ordered to consider the public's right to know in classifying information and were told to use the lowest level of clearance when in doubt. Classification of information was permitted only on the basis of "identifiable" potential damage to national security.

By an Executive Order signed on April 2, 1982, President Reagan reversed each of the critical components of the reforms adopted four years earlier. Government officials were no longer required even to consider the public's right to know when they classified information. When in doubt, Government officials were to classify material at the highest, not lowest, level of secrecy. The requirement that potential harm to national security be "identifiable" was abandoned.

The third step was taken on March 11, 1983. That day, a Presidential directive was issued, requiring a wide range of additional present and former Government officials to obtain clearance from the Government before publishing material that might be classified. The Justice Department document detailing the directive cited the Snepp decision as the basis for the requirement.

The new Presidential order and the Aug. 25 "agreement" released by the Administration that implements it establish a category of information described as "sensitive compartmented information" (S.C.I.) — classified information that is "subject to special access and handling requirements."

Richard K. Willard, Deputy Assistant Attorney General, has defended the Presidential directive by saying that the "prepublication review program provides a reasonable method of preventing disclosures by those employees who have had access to the most sensitive kind of classified information."



A scene from "The Killing Ground," an ABC television documentary.

the directive, prepublication review will be required of all books (fiction or nonfiction), newspaper columns, magazine articles, letters to the editor, pamphlets and scholarly papers by officials with access to S.C.I. materials, so long as what is written describes activities that relate to S.C.I., classified information from intelligence reports, or "any information" — classified or not — "concerning intelligence activities, sources or methods."

Under the new policy, there is no need to submit for prepublication review material consisting "solely of personal views, opinions or judgments" on topics such as "proposed legislation or foreign policy." But the Catch-22 is this: If the opinion even implies "any statement of fact" that falls within the range of review, then the material must be cleared by the Government before it is published. Since most opinions worth expressing about American defense or intelligence policies at least imply some proscribed facts, what the new requirement amounts to is a massive intrusion of the Government into the right of former officials to speak and of the public to listen.

Responding to the initial announcement in March, the Society of Professional Journalists, Sigma Delta Chi, called the directive an "ill-conceived proposal" that is "as troubling as it is sweeping.... Taken with previous actions by the Administration to stem the flow of Government information to the people, the cumulative effect is a major retreat from this country's commitment to open government."

So breathtaking is the scope of the Presidential directive that if it had been in effect before this summer, many articles published in this magazine could not have been printed without prior governmental clearance. An article last year by Gen. David C. Jones, former chairman of the Joint Chiefs of Staff under Presidents Carter and Reagan, criticizing the current defense establishment, would have had to be cleared by the very establishment General Jones was denouncing. This year, ten articles — one by Earl C. Ravenal, a Defense Depart-

'A LESS-KNOWN aspect of the new era of secrecy has pitted the Administration against much of the country's university community.'

ment official under President Johnson, urging withdrawal of American forces around the world, and the other by Leslie H. Gelb, the national-security correspondent for The New York Times who had served in the Johnson Administration, on arms control — criticized policy decisions made by those who would be reviewing them.

The effect of the directive is this: Those people most knowledgeable about subjects of overriding national concern will be least able to comment without the approval of those they wish to criticize.

CHANGES IN LAW TO ASSURE THAT FAR MORE information will be kept from the public are only one aspect of the Reagan Administration's new era of secrecy. Another, far less known, has pitted the Administration against much of the country's university community.

From its first days, the Administration has been concerned that the fruits of American technology have been flowing too freely abroad. "Publication of certain information," complained Adm. Bobby R. Inman, then deputy director of the C.I.A., "could affect the national security in a harmful way." Deputy Secretary of Defense Frank C. Carlucci similarly warned that the Soviet Union was engaged in an "orchestrated effort" designed to gather the "technical information required to enhance its military posture."

The problem that has been vexing the Administration has not been one of classified information. To avoid governmental interference in the open exchange of views at universities, many leading universities have refused to engage in any classified research. The problem has been with material that is not classified at all.

Only a month after President Reagan took office, the president of Stanford University, Donald Kennedy, forwarded a letter to Secretary of State Alexander M. Haig Jr., Secretary of Defense Casper W. Weinberger and Secretary of Commerce Malcolm Baldrige. Written by Dr. Kennedy and the presidents of California Institute of Technology, Massachusetts Institute of Technology, Cornell University and the University of California, the letter expressed concern about Administration interpretation of two statutes.

The university presidents observed that the International Traffic in Arms Regulations and the Export Administration Regulations, which had "not until now been applied to traditional university activities," seemed about to be interpreted so as to inhibit or bar the exchange of unclassified information, the publication of such material, as well as its use in classroom lectures when foreign students were present.

"Restricting the free flow of information among scientists and engineers," the university presidents urged, "would alter fundamentally the system that produced the scientific and technological lead that the Government is now trying to protect and leave us with nothing to protect in the very near future."

The Administration's response was made more than four months later in letters from James L. Buckley, Under Secretary of State for Security Assistance, Science and Technology, and Bohdan Denysyk, Deputy Assistant Secretary for Export Administration of the Department of Commerce. Both tried to assuage the concerns of the university presidents. Neither could fully succeed in doing so. Both letters assured the university presidents that no "new" construction of law was being imposed by the Administration, but the letters were so qualified that it remained unclear just what unclassified technical data were



C. Peter Magrath of the University of Minnesota fears a "chilling effect."

deemed by the Administration to be too sensitive to be taught. Meaningful clarification has yet to be received.

What has been received by universities is a series of letters forwarded from the State and Commerce Departments suggesting that ordinary teaching of unclassified materials may be considered an "export" within the meaning of laws barring the exporting of secret technology. If so, the universities might be subject to civil or even criminal sanctions.

In 1981, for example, in a letter similar to that sent to universities around the nation, the then State Department exchanges officer, Keith Powell '24, asked the University of Minnesota to restrict the academic activities of Qi Yulu, a Chinese exchange student, including denying him access in the area of computer-software technology, "to unpublished or classified Government-funded work." Federal law-enforcement officials also visited the university to emphasize the need for the restrictions.

In a blistering response, the University of Minnesota's president, C. Peter Magrath, pointed out to Mr. Powell that since the university refused to accept classified Government research, scholars from China would not have access to any such material. "We have all kinds of unpublished Government-funded research all over the campus," Dr. Magrath went on, "your proposal would restrict him from access to all of it."

Mr. Powell had asked that the Government be informed prior to any visits of Qi Yulu to any industrial or research facilities. "I can only interpret this," wrote Dr. Magrath, "to give us the choice of confining him to the student union or contacting you several times a day about his campus itinerary. . . . Both in principle and in practice, the restrictions proposed in your letter are inappropriate for an American research university." The proposed restrictions, Dr. Magrath concluded, "can only have a chilling effect upon the academic enterprise. . . ."

IF WE ARE
to restrict the spread
of information
because we cannot
guarantee its
harmless effects, we
will have much
restricting to do.'



Jan Paisley, the Irish Protestant extremist, was one of those denied admission to the U.S. under the McCarran-Walter Act.

In one sense, there is a kind of logic to the Administration's position. As Assistant Attorney General Jonathan C. Rose has said: 'Freedom of information is not cost free; it is not an absolute good.'

representative Robert W. Kas-tenmeier, Democrat of Wis-consin, has proposed such legislation.

Still other decisions are within the control of the courts in their role as protectors of constitutional rights. Some aspects of the Reagan Administration's information policy seem highly unlikely to pass First Amendment muster. It is one thing to say that C.I.A. agents such as Frank Snepp must abide by a contract of silence imposed upon them in the absence of prior governmental clearance. It is quite another to say that the First Amendment could conceivably tolerate the sweeping new restrictions on free-

dom of expression of thousands of former Government officials not involved with the C.I.A. Similarly, it seems most unlikely that disclosing unclassified material previously made public can, consistent with First Amendment principles, be made illegal. When those efforts are directed at universities that have historically received the special First Amendment protection of academic freedom to assure the free exchange of ideas, the chances that any prosecution could succeed seem all the less likely.

In other areas, Congress may, and probably should, amend the McCarran-Walter Act to delete the sweepingly discretionary language that has permitted the State Department to deny American audiences the chance to hear and judge for themselves those foreign speakers the Administration deems objectionable. When President Truman vetoed the bill in 1952, he warned that "seldom has a bill exhibited the distrust evidenced here for citizens and aliens alike." History has proved him right.

Congress may, and probably should, also amend the Foreign Agents Registration Act to delete the requirement of labeling foreign films as "political propaganda." Rep-

resentative Robert W. Kas-tenmeier, Democrat of Wis-consin, has proposed such legislation. Similarly, it seems most unlikely that disclosing unclassified material previously made public can, consistent with First Amendment principles, be made illegal. When those efforts are directed at universities that have historically received the special First Amendment protection of academic freedom to assure the free exchange of ideas, the chances that any prosecution could succeed seem all the less likely.

There remains the question of motive. Why has this Administration gone so far, so fast? Why has it adopted new Government-wide policies limiting the dissemination of information without any showing that harm had been caused by policies previously in effect?

One answer may be easily rejected. It is not because harmful leaks of information have increased in recent years. Deputy Assistant Attorney General Willard, testifying before the House Subcommittee on Civil Rights

this spring, observed that "we have never suggested that it's a problem that has increased greatly in severity in recent years. It's always been a problem." The same day that Mr. Willard testified, Steven Gartink, the director of the Government's Information Security Oversight Office (I.S.O.O.) — which is responsible for the security of all executive-branch agencies involved with classified materials — acknowledged that in the past three years only about "half a dozen" leaks had even been reported to his agency.

What, then, has prompted the Administration's exuberant efforts in this area? In part, it is because the Administration seems not to give much more than rhetorical credit to the concept that the public has a serious and continuing interest in being informed.

There is also a matter of tone. Many of the changes in the classification system are the product of anger by the intelligence community at the Carter Administration. I.S.O.O. has explained that one reason the classification system was rewritten was because the rules previously in effect sounded too "apologetic." Changes in language between that of the Carter Administration ("Information may not be considered for classification unless it concerns...") and that of the Reagan Administration ("Information shall be considered for classification if it contains...") were justified as the substitution of "positive" words for "negative" ones.

Beyond this, there lies something far deeper. The Administration is not only generally conservative; its policy is rooted in the concern that Soviet armed might vastly outstrips that of this country and immediately imperils us. With such a world view, claims of national se-

curity seem invariably to outweigh any competing interests.

In one sense, there is a kind of logic to the Administration's position. Assistant Attorney General Jonathan C. Rose, defending that position, has said that "freedom of information is not cost free; it is not an absolute good." Nor can we be sure what the costs will be. We cannot know what Mrs. Allende might have said had she been admitted to the country or what O. Yulu may have learned on the University of Minnesota campus. We can hardly be sure that all unclassified information is harmless information. But if we are to restrict the spread of information because we cannot guarantee its harmless effects, we will have much restricting to do in the future.

We will also pay a high price for doing so. The "system" that produced the scientific and technological lead that the Government is now hoping to protect" has been a basically open one. By threatening the openness of the process by which ideas are freely exchanged, the Administration threatens national security itself.

It also threatens the nature of American society. If the Russian attack on the Korean jet reinforces the Administration's view about Soviet behavior, it also accentuates the differences between the two countries. It is in the nature of Soviet society to suppress information and to punish those who reveal it. It is in the nature of our society to reveal information and to punish those the information indicates should be punished. The Reagan Administration's moves toward a less open society are contrary to our most deeply felt traditions.

There are, as well, long-range risks in the creation of a new and pervasive apparatus of government secrecy. In relatively placid times, the apparatus may seem merely bothersome to those it touches. In less stable times, it can too easily be used to suppress information essential to the self-government of the country.

In the end, our society is based upon the judgment that the free exchange of information, except in those rare situations where openness will clearly lead to harm, is in the public interest. "Sunlight," Justice Louis D. Brandeis wrote, "is said to be the best of disinfectants; electric light the most efficient policeman." ■

EXPLORATIONS

National Security a Decade After Watergate

JOHN SHATTUCK

Not so very long ago the decline and fall of Richard Nixon brought the problems of civil liberties and presidential politics into the living rooms of millions of Americans on an almost daily basis. White House enemies lists, political misuse of the IRS, CIA domestic spying, FBI burglaries, corruption of the judicial process, the waging of secret wars—month after month these and other disclosures poured forth from newspapers, television sets, and congressional hearing rooms until they forced a president out of office, sent some of his subordinates to jail, and confronted the country with a crisis of confidence in its national government.

But it was never entirely clear what the problem was. Was it Richard Nixon? That was how a majority of the House Judiciary Committee saw it, and they were speaking, no doubt, for a majority of the Congress. Was it a problem of the “imperial presidency” taking over powers of the other branches of government until its overreaching finally shook them out of their slumber? That is certainly the way a large body of scholarly opinion has looked at the crisis of the Nixon White House, and no doubt there is much truth to be found here.

But there was another lesson to be learned from the decline and fall of Richard Nixon, and it was all but forgotten as soon as the crisis of August 1974 was over and a new president was installed in the White House. Nixon himself hinted at one of the most difficult problems he had confronted as president when he described his concept of “national security” in a court deposition in Morton Halperin’s wiretap lawsuit in 1976. Halperin had been the victim of a twenty-one-month warrantless wiretap installed on his home telephone when he was a deputy to Henry Kissinger on the National Security Council staff in 1969. The Halperin wiretap—along with taps on sixteen other government officials and journalists—was part of a Nixon White House investigation of supposed leaks of

sensitive information. When Nixon was questioned about the wiretap program, he justified it as follows:

In America, we have the blessing of both security and freedom. What we were trying to do with this [wiretap] program was to maintain security with the least possible infringement upon freedom. It is not always possible to do so. . . . The use of electronic surveillance to enable the United States to conduct a responsible foreign policy, to get all the options and to get the best possible advice and to get the communication with people abroad that we need to have—I believe that for those fundamental reasons this kind of activity was not only right, but from the standpoint of the security of this country I think it was legally right.

Nixon's view of national security had a profound impact on the inhabitants of the White House. In June 1974, for example, one of the minor dramas of Watergate was played out in a Los Angeles courtroom, when Egil Krogh, chief of the White House plumbers, was sentenced for perjuring himself in connection with the burglary of Daniel Ellsberg's psychiatrist. Before imposing sentence, the judge asked Mr. Krogh whether he wished to make any final statement for the record. He said:

I see now . . . the effect that the term "national security" had on my judgment. The very words served to block critical analysis. It seemed at least presumptuous if not unpatriotic to inquire into just what the significance of national security was. . . . The discrediting of Dr. Ellsberg, which today strikes me as repulsive and an inconceivable national security goal, at the time would have appeared a means to diminish any influence he might have had in mobilizing opposition to the course of ending the Vietnam War that had been set by the President. Freedom of the President to pursue his planned course was the ultimate national security objective.

In the eight years since Egil Krogh was sentenced as a White House plumber, the concept of "national security" has undergone considerable growth. After an initial period of post-Watergate reform, national security policies in recent years have generated steadily increasing pressures on traditional civil liberties. A current example is the Intelligence Identities Protection Act, which was signed into law by President Reagan on June 29, 1982. The Act makes it a crime to publish "any information that identifies an individual as a covert agent" of the CIA or FBI—even if the information is unclassified, is a matter of public record, or is derived entirely from public sources. The impetus for the legislation is the understandable desire to protect the lives of intelligence agents overseas, but as

drafted it almost certainly violates the First Amendment's guarantee of freedom of the press.

It is hoped that no president will use the Intelligence Identities Protection Act to try to curb freedom of the press, but the definitions of national security embodied in the Act are so broad that the First Amendment will be under constant pressure. Sponsors say that the statute is aimed at *Covert Action Information Bulletin*, a journal that has used public record information from newspapers and State Department publications to identify CIA agents. The new law could also silence a *New York Times* reporter who writes an article about agents who participate in the CIA's secret destabilization of Chile, or any other journalist or editor who makes a difficult decision to publish lawfully obtained information about intelligence agencies. Although the legislative history of the Act states that it is not intended to apply to investigative reporting, the express language is very broad. The statute does not require a prosecutor to show that a reporter intended to impair foreign intelligence activities by publishing an expose, but only that he had "reason to believe" that identifying an agent would do so. A warning by the CIA—or even general knowledge of the CIA's sensitivity about the subject of an article—may be enough to constitute the required "reason to believe."

In the face of these broad provisions, it is not surprising that many First Amendment scholars have concluded that the Intelligence Identities Protection Act is unconstitutional. For the first time in American history it would penalize the publication of information that is already public, and it would open the way for a new category of censorship. The authors of the new legislation have candidly stated that civil liberties must yield to superior claims of national security. Senator Richard Lugar, Republican of Indiana, put it very bluntly when he said in an interview with the *New York Times*, "I am willing to take risks with regard to all of the [constitutional] protections we have set up. . . . I don't think on a continuum we are going to be able to have both an ongoing intelligence capability and a totality of civil rights protection." Apparently, Senator Lugar was not just speaking for himself, because on March 18, 1982, the Intelligence Identities bill passed the Senate by an overwhelming vote of 90-6. The Senate vote was only slightly more lopsided than the margin in the House of Representatives, which had passed the bill six months earlier, 354-56.

The Intelligence Identities Protection Act is symptomatic of a growing crisis for civil liberties in the area of national security.

The origins of this crisis are both obvious and obscure. They are obvious because it is a clear lesson of our history that international tension often creates a hostile environment for civil liberties. They are obscure because the causes of

tension in the world today can in some measure be found in our own national security policies. The notorious Palmer Raids on tens of thousands of aliens living in the United States after World War I, the internment of Japanese-Americans during World War II, political blacklisting and McCarthyism in the 1950s—these are some of the ugly legacies of earlier periods when the security of the nation was widely perceived to be threatened. Today we live under conditions of international tension and instability unmatched by any other period in our recent history. A relentless series of foreign military and political crises, coupled with the rapidly increasing threat of nuclear war, have combined to create a substantial impetus in the Reagan administration and parts of the Congress in favor of writing a blank check for national security. The result may be the most serious political crisis for civil liberties since the early 1950s.

As we survey the landscape of national security in the Reagan era, the Intelligence Identities bill is only one of the many recent threats to fundamental rights:

- In December 1980 a Washington research institute, the Heritage Foundation, issued a report on U.S. intelligence agencies prepared by several staff members who later became members of the Reagan transition team. The report calls for stepped-up surveillance of dissidents and a revival of federal internal security machinery. The justification: “terrorist cadres” that grow out of “the splinters of dissident or extremist movements” must be tracked “through the cumulative compilation of comprehensive files.” A central point of the report is that “clergymen, students, businessmen, entertainers, labor officials, journalists, and government workers all may engage in subversive activities without being fully aware of the extent, purpose, or control of their activities.”

- In January 1981, Strom Thurmond, the incoming head of the Senate Judiciary Committee, created a new Subcommittee on Security and Terrorism, to be chaired by Jeremiah Denton, a freshman Alabama Republican, eight-year prisoner of war in North Vietnam and one-time proponent of capital punishment for adultery. In a private comment, a liberal senator paraphrased Roosevelt in 1933, saying, “we have nothing to hope for but fear itself.”

- In April 1981, President Reagan conferred pardons on two former FBI officials convicted of planning and supervising warrantless FBI break-ins of private homes during the search for members of the Weather Underground in the 1970s. The president saluted the two convicted FBI burglary supervisors as “men who acted on high principle to bring an end to the terrorism that was threatening our nation. . . . Their actions were necessary to preserve the security interests of our country.” In response to criticism, the White House issued a statement saying that the President believes “warrantless searches in the intelligence field should be permitted when interests of national security so require.”

- In December 1981, Reagan signed a new executive order on intelligence agencies. It includes new authority for the CIA to mount “covert operations” in-

side the United States so long as they are “not intended” to influence “U.S. political processes,” new authority for the CIA to spy on Americans at home and abroad in order to collect “significant foreign intelligence,” and new authority for the Attorney General to open mail without a judicial warrant if the targets are suspected of being “foreign agents,” a term which is nowhere defined in the order. This new executive order strips away basic civil liberties protections without any public debate.

- Three months later a massive expansion of the security classification system was put in place by the Reagan administration that enshrouds the uses of these new intelligence powers in permanent secrecy. The new classification order tells bureaucrats in essence: “When in doubt, keep it secret.” Gone is the requirement in the Carter administration’s earlier executive order that some “identifiable damage” must be likely to occur if information is not kept secret, as well as the requirement to balance the public’s right to know against the need for secrecy.

- At the same time the Reagan administration began pressing Congress to obliterate key sections of the Freedom of Information Act and CIA officials began urging private scientists to submit sensitive research plans to the government for “preclearance” so that the fruits of their research could be classified and kept secret from foreign governments.

These maneuvers by the Reagan administration have helped foster a climate in Congress where the very words “national security” serve to “block critical analysis.” The effect on civil liberties can be seen by the fact that there are now 158 members of the House of Representatives cosponsoring a resolution to resurrect the notorious House Un-American Activities Committee. It can also be seen by the fact that an obscure right-wing Virginia congressman, Dan Daniel, was able, in late 1981, to tack a rider on a 1982 appropriations bill that harks back to the McCarthy era by barring “communists, terrorists, and subversives” from participating in Labor Department employment programs. The measure was later struck down as unconstitutional by a federal court.

How did we come to this turn of events? The underlying crisis in the presidency of Richard Nixon was the clash between claims of national security—often cynically invoked by the White House—and traditional values of American liberty. But in the presidency of Ronald Reagan, there is little resistance to claims of national security, despite the fact that similar assertions were routinely questioned and sometimes condemned a decade earlier. What happened? The story begins long before Watergate.

At the end of World War II the United States was jolted out of its traditional isolation from world politics and became an active participant and frequent intervener in international affairs. The Cold War that prompted this fundamen-

tal policy-shift appeared to require a permanent place for many of the temporary institutions and powers of wartime mobilization. Just as the executive powers and agencies that had grown up in response to the Depression became a permanent feature in the political landscape during the New Deal, the security policies and intelligence community that grew out of World War II became a permanent feature of the Cold War. Five years after the end of World War II, President Harry S. Truman, with varying degrees of congressional concurrence, had already issued a series of executive orders creating a secrecy classification system, imposing loyalty and security investigations on government employees, and requiring members of the Communist party and other "subversive organizations" in the United States to register with the government. The cumulative impact of these developments on civil liberties reaffirmed James Madison's comment to Thomas Jefferson in 1798 that "perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger, real or pretended, from abroad."

Deep involvement in foreign political and military affairs became the principal feature of postwar American foreign policy. The consequences for the structure of government in the United States were far reaching. For one thing, an interventionist foreign policy served to diminish the power of Congress and to increase that of the executive branch. During this period, Secretary of State Dean Acheson was fond of quoting Tocqueville's warning that "foreign politics demand scarcely any of those qualities which are peculiar to a democracy. . . . [A democracy] cannot combine its measures with secrecy or await their consequences with patience. These are qualities which more especially belong to an individual or an aristocracy." In the United States this precept translated into a strong executive bureaucracy.

The postwar growth of the executive branch had an increasingly distorting effect on the Constitution. The premise of the founders that Congress makes the laws and the executive branch carries them out was a major obstacle to presidents seeking to shape world events to conform to their view of American security interests. Under the Constitution, of course, it is the Congress, not the president, that has the power to declare war, raise armies, and has the final say in the making of treaties. But these arrangements were increasingly seen as a hindrance to quick presidential responses to the long series of foreign crises over the last four decades—Greece, Iran, Lebanon, Guatemala, the Congo, Cuba, the Dominican Republic, Vietnam, Laos, Cambodia, Chile, Angola, El Salvador, Nicaragua—a list that extends to every corner of the world. Hanging over each of these crises like the sword of Damocles has been the confrontation between the U.S. and the Soviet Union and the nuclear balance of terror that has dominated American defense and foreign policies since 1945.

This, then, is the national security framework within which postwar presi-

dents have sought "the freedom to pursue [their] planned course of action." To make up for their lack of constitutional authority to act so freely, every president since Truman has relied on two doctrines to justify executive initiatives to protect national security: inherent presidential power and post-hoc congressional ratification. Taken together, they provide a new legal system within which presidents have felt justified in acting outside the confines of the Constitution.

In the case of inherent power, repeated presidential acts of warrantless wiretapping or covert manipulation of foreign governments are said to validate claims of presidential authority to perform these acts. The Supreme Court rejected the theory of inherent presidential power in its 1952 decision in the *Steel Seizure Case*, when President Truman sought to nationalize the steel industry. But Justice Jackson's frequently cited concurring opinion in that case left the door open to future presidents by recognizing a grey area where the president may act in the absence of express constitutional authority, unless and until the Congress tells him to stop.

In the case of post-hoc ratification, military or intelligence initiatives by the executive branch, even if secret, are said to be tacitly ratified by Congress when it votes general appropriations, as in the case of the secret bombing of Cambodia in 1969 or clandestine efforts to overthrow the government of Chile in 1973. Broad language in congressional statutes, such as the provision in the National Security Act of 1947 giving the CIA director power to "protect intelligence sources and methods," is also said to ratify programs of doubtful constitutionality, such as the CIA's requirement that former employees submit manuscripts for pre-publication censorship.

These doctrines of expanded presidential authority have become the major building blocks of national security policy. They are also major roadblocks for the Bill of Rights.

The national security powers of the president are powers to act in peacetime as if the country were at war. But since at least 1945 we have lived in a twilight zone in which the distinctions between war and peace are so blurred, and the instability of the world so constant that presidents have lacked any objective guideposts for the exercise of their national security powers. "War is peace," wrote Orwell. This maxim has guided presidents for more than thirty years, all of whom have claimed that in order to keep the peace abroad it has been necessary for them to do things at home that, it was once believed, could be done only in a state of declared war.

Nowhere is this more evident than in the areas of government secrecy and political surveillance. Here, the Nixon administration stands out from other recent presidencies only because of the fate of its principal, not because its policies

presented a unique threat to civil liberties. In fact, the development of a law of secrecy and surveillance, and its steady erosion of the First and Fourth Amendments, has accelerated in the post-Nixon, post-Watergate era.

Until 1971 the national security secrecy system had been created and maintained by the executive branch alone. The only law establishing the system was a series of executive orders issued by Presidents Truman, Eisenhower, Kennedy, and Nixon. There were security clearances and investigations in many government agencies, and millions of pages of classified documents. But there was no systematic enforcement of secrecy and no stamp of approval by the courts or the Congress. All that began to change when the Nixon administration went to court in May 1971 to try to block the *New York Times* from publishing the Pentagon Papers. Although the case is widely regarded as a victory for freedom of the press, the Pentagon Papers litigation actually set in motion the development of a formal law of national security secrecy. The case marked the first time the courts had become involved in defining and enforcing the secrecy system; the first time a president had sought the help of the courts in obtaining a prior restraint of publication of the press; and the first time the Supreme Court had said that both the president and the Congress may have authority to restrain the press in this area, although not in that case.

The Supreme Court's 6-3 decision in the Pentagon Papers case was remarkable for the opportunity it gave the president to curtail First Amendment rights at the very moment that it authorized the *New York Times* to roll its presses. Forty years earlier, in *Near v. Minnesota*, another celebrated prior restraint case to come before the Supreme Court, the Court had made it clear that, at least in peacetime, the First Amendment rule against prior restraints is absolute. In times of war, it said, publishing a narrow category of military information might conceivably be restrained if it concerned such details as "the sailing dates of transports or the number and location of troops."

In the Pentagon Papers decision, the Supreme Court abandoned the wartime limitation articulated in *Near*. The pivotal concurring opinions of Justices Stewart and White for the first time generalized the category of information subject to prior restraint and recognized the authority of Congress to legislate in this sensitive constitutional territory. After the dust had settled, the Nixon administration and its successors began to claim that the Pentagon Papers decision had actually established two key principles in a new law of secrecy: first, that the government can block publication of information if its disclosure will "surely result in direct, immediate, and irreparable damage to the nation," as Justice Stewart put it; and second, that if Congress passes a statute authorizing prior restraint, the standard for obtaining an injunction to stop publication can be even lower.

The cat was out of the bag. A succession of post-Watergate cases transformed it into a tiger with a ravenous appetite for the First Amendment. The most spec-

tacular prior restraints to be imposed in the decade since the Pentagon Papers decision involved former employees of the CIA whose writings the government claimed the right to censor. Because former employees are insiders who once had authorized access to classified information, the government argued successfully in these cases that it did not have to satisfy the Pentagon Papers standard in order to obtain a prior restraint. The Victor Marchetti and Frank Snepp decisions established the legal principle that the CIA and presumably other government agencies as well can bar a current or former employee from publishing "any information or material relating to the agency, its activities or intelligence activities generally, either during or after the term of [his or her] employment . . . without specific prior approval of the agency." This new principle is based on the law of contract—if you work for an agency that operates within the national security secrecy system, your employment contract obliges you to waive *permanently* your First Amendment rights to speak and publish without prior restraint.

In Frank Snepp's case this principle was taken to its most Draconian extreme by the Justice Department in the Carter administration. Unlike Marchetti, Snepp was not alleged to have disclosed any classified information in his book, *Decent Interval*, a critical review of the CIA's conduct during the U.S. withdrawal from Vietnam. But the Carter Justice Department sued Snepp to recover the profits he had earned from his book for violating what it called a "fiduciary obligation" to submit the manuscript for CIA clearance, even though Snepp's contract barred him only from disclosing classified information. When the case reached the Supreme Court in February 1980, the Court upheld this new prior restraint theory, 6-3, without even hearing argument, and relegated its discussion of Snepp's First Amendment defense to a footnote of the opinion.

The Snepp litigation was just part of the Carter administration's curtailment of freedom of the press on the grounds of national security. In 1979 the Justice Department moved against a left-wing magazine in an effort to block it from publishing information that was already in the public domain. The *Progressive* case involved an article written about the hydrogen bomb based on information obtained by its author, Howard Morland, from studying government publications. In its effort to obtain an injunction, the government argued that information about atomic weapons is "born classified" and can be restricted under the Atomic Energy Act whether or not its disclosure would meet the Pentagon Papers standard. Although the government eventually abandoned the *Progressive* case when it became increasingly clear that the H-bomb information was not secret, the theory put forward by the Justice Department was that there are whole categories of "dangerous information" that are beyond the reach of the First Amendment.

Three years later, in 1982, the Reagan administration is using this same theory in its well publicized effort to persuade academic scientists to submit their

research plans to the government for clearance. On March 30 the *New York Times* reported that Lawrence J. Brady, Assistant Secretary of Commerce for Trade Administration, condemned what he called "a strong belief in the academic community that they have an inherent right to . . . conduct research free of government review or oversight." So much for the First Amendment.

National security secrecy presents its gravest threat to the First Amendment when it is armed with the criminal law. For this reason it has never been a crime simply to publish information relating to the national defense. Until the enactment of the Intelligence Identities Protection Act in 1982, the espionage laws of the United States applied only to situations in which information was *secretly* passed to a foreign government for the specific purpose of injuring the United States. Even at the height of the Cold War, Congress declined to make it a crime to publish national defense information when it enacted the Internal Security Act of 1950, which expressly provides that "nothing in this Act shall be construed to authorize, require, or establish military or civilian censorship."

In 1971 this consensus began to break down when the Nixon administration, on the eve of oral argument in the Pentagon Papers case, indicted Daniel Ellsberg for releasing the papers to the press. In pursuing the Ellsberg prosecution before it was dismissed because of government misconduct, the Nixon Justice Department argued that there was no need for it to show that Ellsberg intended to damage the United States, and that it did not matter that he had passed the papers to the *New York Times*, rather than to a foreign government. All that mattered, the Justice Department said, was that the papers were the property of the government and that Ellsberg knew they were classified.

Seven years later, in 1978, this same theory was successfully used by the Carter administration when it obtained convictions of Ronald Humphrey and David Truong in a celebrated espionage prosecution. Humphrey and Truong had been charged under the espionage statute with passing national defense information to persons not entitled to receive it, without any allegation that they had done so with an intent to injure the United States or even that they had passed the information to agents of a foreign government. Soon after the Truong and Humphrey convictions, the Carter administration sent to Congress the first version of the Intelligence Identities Protection Act, reflecting all the elements of the new crime of disclosing official secrets. Although it took the Reagan administration to secure the bill's enactment, the new crime had been planted and carefully nurtured by three presidents.

Like the law of secrecy, the law of national security surveillance has evolved from bold presidential assertions of power to an extensive authority ratified by judicial decisions and congressional enactment. Every president since

Franklin Roosevelt has claimed the power to conduct warrantless wiretapping of foreign governments. But once again, it was Richard Nixon who put forward the most sweeping claims in this area, and sought to have them approved by the courts.

In a series of cases beginning in 1969, the Nixon administration argued that it had an inherent power to disregard the Fourth Amendment warrant requirement whenever it conducted wiretaps or physical searches of persons or groups believed to be a threat to the national security. In the first such case to reach the appellate level, this argument was rejected by the Sixth Circuit Court of Appeals, which wrote a scathing opinion in 1971 comparing the Nixon claims to the royal prerogatives of King George III to search the houses of colonists—prerogatives whose exercise triggered the American Revolution and were foremost in the minds of the Founding Fathers when they wrote the Fourth Amendment to the Constitution prohibiting unreasonable searches and seizures. The Sixth Circuit decision was affirmed by a unanimous Supreme Court in 1972. Like the Pentagon Papers decision, however, the Court's ruling in the national security wiretap case was most significant for what it did *not* decide. Since the wiretap at issue had been installed on a domestic organization with no connections to any foreign power, the Court left open the possibility that warrantless surveillance of a person or group with "foreign ties" would be legal. For the next few years, however, the erosion of the Fourth Amendment appeared to have been contained.

By the end of the Nixon administration, the courts and the Congress were viewing presidential claims of national security with skepticism. In a 1973 Freedom of Information Act case, for example, when a group of congressmen sued the Environmental Protection Agency to obtain information about the environmental impact of underground nuclear testing in Alaska, several Supreme Court Justices observed in a concurring opinion that blanket national security claims can be "cynical, myopic, or even corrupt." A year later, the Watergate tapes case provided a dramatic example of such a claim.

But the political corruption of the Nixon White House obscured the steady development of a new law of national security surveillance. Taking its cue from the Supreme Court's 1972 wiretap decision, the law began to focus on the elusive concept of "foreign agency." Since the Court had held that the Fourth Amendment only barred warrantless national security surveillance of domestic targets, suspected agents of a foreign power were presumed to be beyond its reach. Ironically, this distinction established a legal rationale for much of the surveillance that had been condemned in the Nixon era. One example was the CIA's program of spying on the anti-Vietnam War movement, jauntily dubbed "Operation CHAOS." This was a surveillance effort to ferret out links between the leaders of the peace movement and foreign governments. Although no such links were ever established, the program resulted in the creation of CIA files on more than

300,000 domestic activists participating in activities that had been under suspicion for having a foreign stimulus.

The Ford, Carter, and Reagan administrations have all claimed, in a series of executive orders, that undefined foreign agent surveillance is beyond the reach of the Fourth Amendment. The confusing world of these executive decrees is best captured by a section of the Carter order entitled "Restrictions on Certain Collection Techniques." It reads as follows:

Activities . . . for which a warrant would be required if undertaken for law enforcement rather than intelligence purposes, shall not be undertaken without a judicial warrant, unless the president has authorized the type of activity involved and the Attorney General has both approved the particular activity and determined that there is probable cause to believe that the United States person is the agent of a foreign power.

What does this mean? It means that whenever the government has "probable cause to believe" that a person in the United States is an "agent of a foreign power" (a term not defined in the executive order), that person can be targeted for unlimited, warrantless wiretapping, television monitoring, physical searches, and mail opening. A White House document further explaining and implementing this claim of presidential power is classified "because of the sensitivity of the information and its relation to national security."

The Ford, Carter, and Reagan executive orders on intelligence agencies have been issued with much public fanfare proclaiming the "rule of law" over the "intelligence abuses" of the Watergate era. At the same time, however, the orders have been broadly drafted to fit the needs of the national security apparatus, regardless of their impact on civil liberties. The Reagan order represents the culmination of this process. It goes beyond the "foreign agent" approach of the Carter administration and authorizes the CIA to conduct general surveillance of anyone inside the United States who may be in possession of "significant foreign intelligence," such as journalists or academics or businessmen returning from trips overseas. It also authorizes the CIA to conduct undefined covert operations inside the United States so long as they are not "intended" to influence "the political process, public opinion, policies or the media." No secret abuses can occur now. Everything is out in the open. All in black and white. All within the claim of a general foreign security loophole to the Constitution.

During the last decade there has been only one successful effort in the Congress to narrow this presidential claim, and that success has been mixed. In 1978 Congress enacted the Foreign Intelligence Surveillance Act, requiring judicial warrants based on evidence of criminal conduct for most national security wiretapping in the United States. On paper, this statute is a significant improvement

over the chaotic state of the law before its enactment. It puts Congress on record against presidential claims of inherent power to conduct unrestricted surveillance, and it all but closes the "foreign security" loophole to the warrant requirement left open by the Supreme Court in its 1972 decision. On the other hand, the statute authorizes the executive branch to keep all its foreign security wiretaps permanently secret, and it lowers the standard for the issuance of warrants so that full-fledged probable cause of a crime does not have to be shown.

The real significance of the Foreign Intelligence Surveillance Act, however, will ultimately depend how it is applied. The early signs are not encouraging. The statute sets up a special "Foreign Intelligence Surveillance Court" to receive applications for wiretap orders. The court operates under extraordinary security procedures for the handling of materials submitted to it—procedures that inevitably compromise its independence from the executive branch. So compelling is the lure of legitimacy surrounding this special court that the Carter administration could not resist turning to it on at least three occasions in 1979 and 1980 for approval of physical searches as well as wiretaps, paving the way for routine cooperation between the executive branch, the courts, and the Congress in pruning back the Constitution in the name of national security. In essence, the Carter Justice Department was saying that since Congress has created a special national security court, that court should be used as an all-purpose source of authority for particular executive actions curtailing constitutional rights. If the court can authorize wiretaps, why not physical searches, mail opening, covert action, prior restraint, and censorship?

Apparently the Reagan administration prefers to leave these delicate matters to executive discretion, so the Foreign Intelligence Surveillance Court is once again limited to performing its statutory function of serving up wiretap warrants that their targets will never see. But the new court is a permanent feature of our legal system and it stands for the stark proposition that the conflict between constitutional rights and national security must be adjudicated under different procedures than those which apply to other areas of constitutional law.

The development of a formal law expanding the concept of national security is a largely unnoticed legacy of the Watergate era. Out of the national trauma that accompanied the impeachment proceedings against Richard Nixon there emerged a consensus that abuses of presidential power must be contained by the rule of law. This consensus was best articulated by Chief Justice Warren Burger, speaking for a unanimous Supreme Court in the White House tapes decision, which served as Nixon's writ of execution in July 1974:

The President . . . reads the Constitution as providing an absolute privilege of confidentiality for all presidential communications. Many de-

cisions of this Court, however, have unequivocally reaffirmed . . . that it is the province and duty of the judicial branch to say what the law is. . . . We conclude that . . . the [President's] generalized assertion of privilege must yield to the demonstrated, specific need for evidence in a pending criminal trial.

But the rule of law has little force if the law can always be bent by claims of necessity. Another passage from Burger's opinion in the tapes case is a reminder that the consensus about Nixon's abuses of power never touched his claims about the necessities of national security. How much deference should be accorded to presidential definitions of national security? The view of the Court is that few questions should be asked of a president when he claims to be acting in this area.

The President does not place his claim of privilege on the ground that [the tapes] are military or diplomatic secrets. As to these areas . . . the courts have traditionally shown the utmost deference to presidential responsibilities.

National security is a ubiquitous concept that presidents have frequently invoked over the last three decades to insulate their actions from review. The law has not only been inadequate as a safeguard against overreaching claims of national security; it has become, especially since the Nixon presidency, a source of legitimacy for the view that definitions of national security should be left to the discretion of the executive branch. Over the last eight years the courts and the Congress have increasingly been drawn into the conflict between security and liberty, but instead of defining and narrowing security claims by the executive branch, they have often ratified executive practices and insured them against legal challenge.

The ultimate effect of much law in this area has been to authorize discretion and flexibility in the management of security practices. The result is that today we have greater secrecy, more censorship, a CIA with more domestic authority, an FBI with fewer restraints, and a National Security Agency with broader power than we have ever had in our history. And all of these developments have taken place under a new system of law that has grown up in the shadow of the Nixon presidency, after we thought we had struck down the abuses that produced Watergate. Ten years later, most Americans are not aware of this continued erosion of their individual liberties in the name of a dangerously expanding concept of national security.

What is most remarkable about all this is that we have drifted into a state of permanent emergency that has no immediate contest. We do not know what the emergency is or how long it will last. We do not even have a clear understanding of its impact on our system of liberty, since we have been conditioned to accept

the view that the rule of law often requires individual liberty to yield to claims of security under certain limited circumstances. In fact, we do not even think of ourselves as living in a state of emergency. On the contrary, we believe that a general suspension of liberty happens only in other countries and could never happen here.

Take a typical example close to home. On October 16, 1970, Prime Minister Pierre Elliott Trudeau went on Canadian national television and declared a "state of insurrection" throughout Canada, based on the kidnapping of a Canadian minister and a British consul by Quebec separatists. Trudeau invoked the Canadian War Measures Act and authorized the national police to conduct predawn roundups of French Canadians suspected of associating with the separatists. Trudeau's emergency decree had the effect of temporarily suspending the Canadian Bill of Rights.

Could it happen here? Probably not the way it happened in Canada. We are not likely to experience such a dramatic announcement and clear suspension of the Constitution in a time of similar crisis. Why not? Because our law of national security is flexible enough to accommodate almost any necessity. A decade ago, the Nixon administration was already able to devise methods of coping with similar emergencies without formally suspending the Constitution. In 1971 Nixon's second attorney general, Richard Kleindienst, commented on Trudeau's declaration of emergency by stating:

It could not happen here under any circumstances. We wouldn't suspend the Bill of Rights even if the whole Cabinet, the Chief Justice and the Speaker of the House were kidnapped. . . . We wouldn't have to because our existing laws—together with our surveillance and intelligence apparatus, which is the best in the world—are sufficient to cope with any situation. . . . There is enough play at the joints of our . . . law, enough flexibility, so that if we really felt that we had to pick up leaders of a violent uprising, we could. We would find something to charge them with and we would hold them that way for a while.

That, of course, is exactly what the Nixon Justice Department did when it unceremoniously rounded up 12,000 people in the streets of Washington, D.C., during the May Day antiwar demonstrations in 1971. Although these mass arrests were later condemned by federal courts as unconstitutional, they were an awesome display of informal executive power to define and declare emergencies and suspend the Constitution. Comparing the Canadian and American approaches to national security, the Canadian Attorney General, John Turner, made a wry comment after Trudeau lifted his emergency decree:

In a certain sense, it is a credit to the civil liberties of a country that it has to invoke extraordinary powers to cope with a real emergency. Some

countries have these powers at their disposal all the time.

Is the United States becoming such a country? Without clearly defining what we mean by national security, we have turned it into a talisman to ward off any evil that might befall us as a nation. It is disturbing, but not surprising, therefore, that the current administration has turned the CIA loose to spy on Americans and conduct "covert actions" inside the U.S.; created a presumption that all government information about foreign or military affairs can be withheld from the public; pardoned FBI officials who supervised criminal burglaries as heroes in a war against terrorism; mounted a campaign for official censorship of scientific research; and accused the critics of its foreign policy of promoting Soviet propaganda.

There is a simple question that we must ask ourselves as we look at these recent developments and the long history of national security maneuvers that preceded them: where does the Constitution fit in? National security is what protects us from our adversaries, but the Constitution and the Bill of Rights are what distinguish us from them. The question, of course, is not just one of law. We must decide what we mean by national security and whether its protection should be allowed to blur our principal distinguishing features as a nation. "Liberty lies in the hearts of men," Judge Learned Hand said in a famous speech delivered during a time of grave national danger, in 1943. "When it dies there, no constitution, no law, no court can save it." Judge Hand's speech echoed the warnings of the drafters of the Bill of Rights that, in the words of Thomas Paine, "those who expect to reap the blessings of freedom must always undergo the fatigue of supporting it."

John Shattuck is national legislative director of the American Civil Liberties Union and head of its Washington Office. This article is reprinted by permission from the Winter 1983 issue of *democracy*, "a journal of political renewal and radical change."

Faculty Opinion

New Report Spring 1984

Professor Emerson, Lines Professor Emeritus of Law at Yale, delivered these remarks when he accepted the First Amendment Defender Award presented to him in December 1983 by the Institute for Communications Law Studies of the Catholic University School of Law in recognition of his lifelong efforts to preserve and strengthen First Amendment protections. The remarks were published in *Communications Lawyer* (Winter 1984) and are reprinted here with permission.

In addition to being the first recipient of the First Amendment Defender Award from the Institute of Communications Law Studies, Mr. Emerson has recently received two other distinguished awards. The American Civil Liberties Union has awarded Mr. Emerson the first ACLU Medal of Liberty for distinguished lifetime service to the cause of civil liberties. The ACLU hopes the Medal will come to represent the pinnacle of achievement for those dedicated to the grand purposes of the Bill of Rights. It is the only award the national ACLU confers. Secondly, the Connecticut Bar Association has honored Mr. Emerson with the 1983 Distinguished Public Service Award for "exercising freedom of expression in the cause of everyone's freedom of expression."

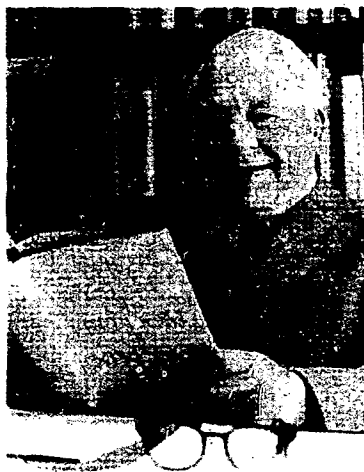
The State of the First Amendment As We Enter "1984"

Thomas I. Emerson

When the First Amendment became a part of the Constitution in 1791 the scope and implications of that provision were by no means clear. Its fundamental purpose was to support the principles of an open and self-governing society. More specifically, it was intended to protect speakers who criticized the government, to forbid censorship of the press, and to permit assemblies in the public halls or demonstrations on the streets. But many questions remained unanswered, such as its effect upon the law of seditious libel, private libel, blasphemy, obscenity, and advocacy of law violation. Even the issue of who was protected by its terms was not beyond dispute. Moreover, the guarantee did not apply to the states. Thus the First Amendment had a vast potential—it was indeed a daring innovation—but its future was uncertain.

For well over 100 years there was little or no development by the courts of First Amendment doctrine. Some right to freedom of expression existed in practice. But the right was subject to frequent infringement, including prosecutions under the Alien and Sedition Acts, molestation of abolitionists, and disruption of IWW meetings. Yet not until World War I did the issues come before the Supreme Court in a serious way. And not until 1925 was the First Amendment made applicable to the states, where most of the abridgements of the right of free expression were occurring.

In the last five or six decades, however, there has been a tremendous development of First Amendment law. Fortunately, the Supreme Court and other courts, despite some argument to the contrary, have interpreted the First Amendment as part of a living constitution.



They have broadly accepted the basic principles embodied in the First Amendment and carried the application of those principles far beyond the immediate areas the framers apparently had in mind. The result has been the creation of a constitutional structure that supports a relatively strong system of freedom of expression. That system, flawed as it is in many respects, has had a global impact and constitutes a major contribution to the progress of humankind.

Partly as a result of the First Amendment and its accompanying body of law, George Orwell's *1984* has not come to pass in the United States. Nevertheless, serious dangers to the system exist and difficult problems remain to be solved. In appraising these dangers it is necessary to explore, in general terms, the extent to which a basic understanding of the First Amendment prevails in our society and the way in which the supporting constitutional doctrines have been developing. It is also important to take note, albeit very briefly, of some of the specific problems that currently require solution.

Basic Understanding of the First Amendment

Creation of a healthy system of freedom of expression under the First Amendment does not come without travail. As Justice Holmes has said, majorities are prone "to sweep away all opposition." Governments strongly prefer acquiescence to dissent. The long-term benefits of tolerating the views of others are often not immediately apparent. The system, in short, is a

sophisticated one, requiring the education and reeducation of each generation. Ultimately it rests upon a sensitive understanding of the principles at work and a firm commitment to their support.

There are signs in the land that this essential understanding and support is slackening in some quarters. Three areas of concern stand out.

First, the current Administration, from the highest levels on down, has taken a series of actions that can only be premised upon ignorance of, or wanton disregard for, First Amendment values. Thus, although the Freedom of Information Act has been one of the major advances in the democratic process over the past several decades, the Administration has proposed weakening amendments that would drastically curtail its capacity to give the American people information they need to know. The Administration has also denied visas to important foreign visitors, apparently on the theory that their ideas are too dangerous for the American people to hear. It has revived the Foreign Agents Registration Act to require that two Canadian films, one on acid rain and the other on nuclear energy, be labelled "political propaganda"; the point seems to be that the American people must have fatherly advice in order to evaluate materials emanating from foreign sources. In the area of political surveillance, the Administration, despite past disclosures of glaring abuse by the intelligence agencies, has not only failed to bring the intelligence agencies under statutory control, but by executive order and revision of the attorney general's guidelines has sought to undo even the feeble reforms instigated by the prior Administration. And, contrary to past practice, the Administration excluded the press from Grenada during the invasion, thereby leaving the American people without any independent source of information on what was taking place.

The failure of the current Administration to comprehend the elementary principles of the First Amendment is revealed most starkly by its efforts to control the dissemination of scientific information on national security grounds. While secrecy on some matters affecting national security is essential, the Administration has gone much beyond reasonable precautions. Using the export control laws it has imposed far-reaching restrictions on the teaching and research activities of American universities and scientists. Thus, it has undertaken to control the publication of research materials, even where they do not deal with classified information, to monitor the study of foreign students in American universities, and generally to hinder communication between American and foreign scientists. One example of the Administration's

activities occurred in August of last year when, at a conference in San Diego of 2,700 photo-optical engineers, the Department of Defense blocked the presentation of 100 papers containing nonclassified information. The Administration seems totally unaware that the scientific method itself—the hope for scientific progress—depends on full freedom of inquiry, the exposure of fact and theory to testing and criticism, building upon the knowledge uncovered by others, and an atmosphere of open dialogue. The Administration's guiding philosophy, to the contrary, leads straight to "1984."

A second area of weakness in the basic understanding essential to a vigorous First Amendment involves what has been called the "pollution" of the market place of ideas. The system of freedom of expression has always operated in a somewhat rowdy fashion. Much that is said is false or misleading, inipugns the motives of the opposition, is intemperate, or appeals to prejudice rather than reason. It is not the province of the government to attempt to purify the process. That could only be done at the price of destroying the system altogether.

Nevertheless, participants in the system do have a moral and political responsibility. Surely there is some obligation to maintain and improve the quality of the debate. Above all it is vital that all of us learn from the mistakes of the past; there should be no need to repeat the blunders of McCarthyism. Hence one must always hope that the content of the system will become more meaningful and more useful to society as a whole.

Unfortunately this does not seem to be happening. Indeed there are ominous signs of contrary trends. Traditionalist forces in the nation, basically opposed to innovation and diversity, have become more articulate, better organized, and politically more powerful. And their area of attention has moved from social issues—the family and religion—to questions of military and foreign policy. Their participation in the system is welcome, but their mode of operation has tended to undermine the First Amendment in at least two ways.

One is that expression of their particular point of view tends to be accompanied by attempts to suppress the viewpoints of others. As Justice Douglas once said, they "demand conformity—or else." This attitude has found expression, for instance, in the efforts to ban books from libraries and schools. Considerable evidence points to the conclusion that the book-banning phenomenon has reached alarming proportions. Thus, last year, according to the Office for Intellectual Freedom of the American Library Association, more than 50 percent of high school libraries responding to a national

survey reported some form of censorship pressure. And a recent study by People for the American Way concluded that censorship efforts have been steadily increasing, with "secular humanism" the most frequent target of the attacks. Book banning is, of course, the essence of "1984."

The other danger to the First Amendment arises from the practice of substituting for a discussion on the merits an attack upon motives or an appeal to fear or prejudice. This mode of exercising First Amendment rights takes the form of questioning the integrity of the opposition, attributing its information or ideas to foreign or other sinister sources, suggesting hidden agendas, proclaiming guilt by association, and generally equating opposition to official policy with disloyalty or even treason. Examples of this approach are seen in much of the response to the nuclear freeze movement, the attack upon the National Council of Churches, and the campaign against the Institute for Policy Studies. In all these cases the very real substantive issues raised by the groups involved were not faced and the public was deprived of an opportunity for national debate.

A third concern with the basic support for the First Amendment in contemporary society arises out of some backsliding on the intellectual front, particularly among some constitutional experts. The attempt by the academic community to formulate rules of law that will give realistic protection to First Amendment rights has not moved forward. On the contrary, theories of limitation are being advanced in some quarters. Thus, proposals to restrict coverage of the First Amendment to "political expression," that is, participation in the affairs of government, are still being pressed. Ideas for downgrading the importance of the rule against prior restraint are being put forward. And arguments that time, place, and manner restrictions are permissible, so long as the regulation is "content neutral," are being urged. One is, of course, not entitled to ask the legal academic community to accept any one approach to strengthening the First Amendment. But a less constrained, and more generous, attitude toward the problem might not be out of place.

The Supporting Constitutional Framework as Fashioned by the Supreme Court

Under our system of government we rely heavily upon the courts, topped by the Supreme Court, to create and maintain a legal structure that will make the protection of First Amendment rights a reality. We count on our judicial institutions to expound the principles, to formulate the doctrines, to apply the rules in new

situations, and generally to enforce the guarantees of the First Amendment against legislative, executive, or popular pressures. The fashioning of an effective body of up-to-date law is a matter of supreme importance in the fortunes of the First Amendment.

In general the Supreme Court has accepted the basic values that underlie the First Amendment and has recognized the functions it was meant to serve in our society. Moreover, in the years since World War I the Court has constructed a substantial set of legal rules, derived from those values and functions, that give solid life to the constitutional guarantee. Yet the dream of a comprehensive and tight-fitting constitutional structure has not been realized. Not only do important differences of opinion persist among the justices, but the rules remain loose and a gradual dilution of doctrine seems to be taking place.

The most fundamental tenet of First Amendment law is that speech or expression, as distinct from other conduct, occupies a special position in our hierarchy of values and is entitled to special legal protection. In other words, in constitutional adjudication speech or expression must be given a "preferred position." The right to freedom of expression cannot simply be balanced away by being made subordinate to other governmental interests. Rather, the other interests must fit within a structure that protects expression, that is, be achieved by means that do not deny or abridge freedom of speech. Although this is the starting point of First Amendment analysis the Supreme Court has wavered on the matter. It has never flatly repudiated the principle, but more and more it has ceased to pay attention to it. Certain of the justices, and sometimes a majority, treat First Amendment rights as merely of passing concern, readily subordinated to any other substantial governmental interest. The special place accorded freedom of expression in our constitutional law seems to be diminishing.

A second fundamental tenet of First Amendment law is that freedom of speech extends to all forms of expression, whether political, academic, artistic or other, and that expression is protected regardless of content, whether racist, sexist, totalitarian, or other. Here the Supreme Court has held firm. It has refused to limit the First Amendment to "political speech" and, in the *Skokie* case, it made clear that even racist speech of the most vitriolic kind came within the protection of the First Amendment.

Beyond this, however, the Supreme Court has not advanced very far in defining just what is expression, and hence entitled to constitu-



tional protection, and what is non-speech or action and not covered by the First Amendment. The Court still adheres to the fiction that obscenity is not expression. It has not found any technique for determining when symbolic speech comes within the purview of the First Amendment. And it has not succeeded in drawing a satisfactory line between militant advocacy and violent action. Hence the question of what conduct is protected by the First Amendment has been left in a state of ambiguity. The result is that expression and action tend to be merged in the Court's analysis and the protection given expression does not rise above that afforded other forms of conduct.

Once having determined that certain conduct is expression within the ambit of the First Amendment, the further question is what degree of protection is constitutionally required. Apart from the advocacy cases, where a test combining clear and present danger and incitement is employed, the Supreme Court relies principally upon the balancing test, attempting to weigh First Amendment values against other interests. The objections to the balancing test have been recounted many times. The difficulties include the fact that there are no comparable factors to weigh against each other, that the formula is so unstructured as to lead to any result, and that the court tends ultimately to look mainly to the government interest involved and ignore the preferred position which ought to be accorded expression. In addition, as the Supreme Court continues to expand its balancing techniques it has come to weigh in the balance

various factors with which the government, under First Amendment theory, ought not to concern itself. Thus the Court has taken to considering the relative value of different forms and different contents of speech, trying to measure the extent of the abridgement of expression caused by the government's action, and permitting a greater degree of government control where other modes of expression are available to the speaker. In utilizing factors of this sort in the balancing process the Court is permitting the government to make judgments as to the social value of different kinds of expression—matters which should not be the business of the government at all.

On another front, the doctrine of prior restraint has been losing some of its force. The Supreme Court still recognizes the drastic impact of advance censorship and the unique character of a prior restraint. But a majority of the Court has been unwilling to formulate general rules forbidding such controls. The result is that the existence of an invalid prior restraint is determined on an ad hoc basis in each case. And the courts have not been adverse to imposing a temporary prior restraint until the final determination can be made. This is what happened in the *Progressive* magazine case, where a prohibition against publication was in effect for nearly seven months until the ultimate issue was resolved.

Nor has the Supreme Court sponsored innovative doctrine in the First Amendment area. Despite the fact that many individuals and groups lack access to the means of communication, the Court has done little or nothing to solve this problem. In fact, on the whole it has narrowed the right of access rather than expanded it. And, although the Court has acknowledged the existence of a public right to know, it has not developed this doctrine in any substantial way.

All in all it can be said that the Supreme Court has maintained a significant body of law supporting the First Amendment. But there are loopholes, ambiguities, and other serious weaknesses in the system. It is by no means sure that a sufficiently hard-shelled structure has been developed to withstand the pressures of a crisis. Nor has the Court moved forward to deal with some of the upcoming problems engendered by the times.

The First Amendment and National Security

Of the specific First Amendment problems confronting the nation on the eve of 1984, perhaps the most significant, and certainly the most urgent, is the reconciliation of national security interests with the principles of the First Amendment. The issues are complex and troublesome.

Preservation of national security is, of course, a basic need of any society. Appeals in the name of national security arouse the kind of popular response that tends to "sweep away" all other considerations. The secrecy surrounding most national security claims makes it difficult for the public to obtain the full facts. Yet, if we are to remain a democratic country we must find a way to fit national security concerns into our system of individual rights.

The tightening circle of government restrictions upon freedom of expression, imposed as requirements of national security, has been described by many observers. Some of these measures have been noted above. One more, which dramatically illustrates the direction in which we are traveling, may be added.

On March 11, 1983, the President issued a Directive on Safeguarding National Security Information. This directive, as implemented by Department of Justice regulations, provides that all persons with access to classified information must sign an agreement that they will never disclose classified or classifiable information related to their government employment. In the case of persons with authorized access to special, so-called Sensitive Compartmented Information, estimated at over 100,000 government employees, the agreement would require also that they submit all future writings related to their government employment, including works of fiction, to the agency for its approval before publication. All classified or classifiable information to which access is made available "is now and will forever remain the property of the United States Government." The agreements are to be enforceable in a civil action for injunction, damages or other relief. In addition the directive instructs every government agency to adopt regulations providing that its employees may be required to submit to polygraph examinations in the course of any investigation of the unauthorized disclosure of classified information. The FBI is given jurisdiction to investigate unauthorized disclosures even when no criminal prosecution is anticipated.

The restrictions imposed by the directive would drastically curtail the flow of information concerning government policies and activities. They would, for example, require a former secretary of state writing his memoirs to submit the manuscript for advance approval by the current secretary of state. It is not too much to say that implementation of the directive, which has been temporarily held up by congressional action, would substantially change the balance of power between the government and the citizenry.

Obviously, these developments raise serious First Amendment issues. Before examining the

recent Supreme Court decisions in the national security area, however, it is important to sketch the broader constitutional landscape.

The starting point is that governmental efforts to achieve national security, like the exercise of all other government powers, must operate within the constitutional structure. More specifically, the goal of national security must be sought by methods that do not infringe First Amendment rights. The government has increasingly contended otherwise. But that position has been consistently rejected by the Supreme Court. Thus, when President Truman attempted to take over the steel mills during the Korean War, on the ground that seizure was necessary to our national defense, the Court ruled that "we cannot with faithfulness to our constitutional system" uphold such action. In *New York Times v. United States* the Court refused to grant an injunction against publication of the Pentagon Papers even though the government claimed it would cause "grave and irreparable injury" to national security. And in *United States v. United States District Court*, decided in 1972, the Court rejected the government's claim that the Fourth Amendment did not apply to wiretapping in domestic security cases. "We recognize the constitutional basis of the President's domestic security role," said a unanimous Court, "but we think it must be exercised in a manner compatible with the Fourth Amendment."

It must be recognized, of course, that national security considerations continue to play a significant role in constitutional adjudication. In the application of constitutional limitations national security factors are frequently relevant. A strong argument can be made for the proposition that, in certain kinds of cases, national security factors can never justify infringement on freedom of expression. Thus in most cases of prior restraint, in cases involving the suppression of information in the public domain, and in cases of political surveillance not related to law enforcement, the First Amendment should automatically carry the day. The Supreme Court has not, however, taken this road. In place of giving the full protection of the First Amendment it has adopted a balancing test. Furthermore, there are some situations, such as control over expression by government employees, where full protection is not possible and resort to balancing becomes necessary.

In any event, by balancing or otherwise, the courts retain substantial leeway to determine whether government efforts to achieve national security conform to constitutional limitations. In that contest between national security and First Amendment rights, the cause of freedom of expression tends to be subordinated. The

heaviest pressures seem to be on the side of national security, and individual rights are too readily balanced away. Under these circumstances a resolution of the issues that gives adequate weight to First Amendment values can be achieved only if the courts adhere to certain equalizing rules. These rules may be stated as follows:

1. Constitutional principles protecting freedom of expression occupy a preferred position in the hierarchy of democratic values; hence, there is a presumption in favor of the constitutional right.
2. Government claims of injury to national security must be viewed with a healthy skepticism.
3. The burden of proof to demonstrate its case for limitation rests upon the government.
4. The government must show a direct, immediate, grave, and specific harm to national security, not just a vague or speculative threat.
5. The restriction sought by the government must be confined to the narrowest possible constraint necessary to achieve the goal, and should not be permitted where methods having a less drastic effect upon First Amendment rights are available.
6. Wherever possible, hard and fast rules, rather than loose balancing tests, should be formulated and applied.

Unfortunately the Supreme Court has not accepted this approach and its recent record in First Amendment-national security cases gives cause for alarm. In the *Pentagon Papers* case the Court was unable to produce a majority opinion, but the least common denominator of six of the opinions rendered would seem to be that the government could enjoin the publication of information whenever it is shown that dissemination of such information would cause a "direct, immediate, and irreparable damage to our Nation or its people," regardless of the extent of the injury or its impact upon freedom of expression. Moreover, a prior restraint can be imposed while that issue is being determined. In *Laird v. Tatum* the Court ruled that a wide-ranging program of political surveillance by Army Intelligence caused only a "subjective chill," insufficient to give the targets of the surveillance standing to challenge the government's action. In *Snepp v. United States* the Court upheld a CIA prepublication secrecy agreement against a former employee who had published a book critical of the CIA even though the book was not alleged to contain any classified information. The Court did not bother to wait for briefs on the merits or to hear oral argument. It treated the prepublication agreement as if it were nothing more than a private contract not raising any issue of the public's right to know.

And it dealt with the First Amendment only in a casual footnote, saying that the agreement exacted of Snepp was "a reasonable means" of protecting a compelling interest. Finally, in *Haig v. Agee* the Court approved a State Department regulation that authorized withdrawal of a passport where the activities of an American citizen abroad "are causing or are likely to cause serious damage to the national security or the foreign policy of the United States." "Matters intimately related to foreign policy and national security," declared a majority of the Court, "are rarely proper subjects for judicial intervention."

Thus, the Supreme Court, far from adopting a set of principles that would give the First Amendment a fighting chance against assertions of national security, has come close to abandoning the effort to assure that constitutional liberties will be taken into account. There is real danger that First Amendment rights will be overwhelmed by national security demands. Such a result need not be. Past experience shows that the dangers to national security from freedom of expression have been vastly overdrawn and that a democratic accommodation can be made. Our traditions also tell us that it is futile to search for total security. National security achieved at the sacrifice of our system of individual rights is not national security in any true sense.

The First Amendment and the Changing Technology

A second major problem for the First Amendment—or rather series of problems—arises out of the vast changes taking place in the technology of communication. When the First Amendment was drafted at the end of the eighteenth century the chief form of expression consisted of the printed press, meetings, demonstrations, and the like. During the course of this century radio and television came to play a prominent role. At the present time the system of freedom of expression is being revolutionized by the development of radically new modes of communication. These include cable television, satellites, microwaves, optical fibers, computers, facsimile, videotapes, and many similar devices. Two aspects of this new technology are of paramount importance for the future of the First Amendment. One concerns the breakdown of the traditional differences in First Amendment law between the print media and the electronic media. The other is the potential for wider access, by diverse individuals and groups, to the mass media.

As First Amendment law has developed there has emerged a significant difference in the degree of governmental control allowed over

the traditional print media and the newer electronic media. The older forms of communication enjoy, at least in theory, a somewhat higher degree of protection from governmental interference. Restrictions upon the content of the communication, with some exceptions for libel, obscenity, advocacy of law violation, and the like, are forbidden. Time, place, and manner controls are limited, by and large, to those necessary to provide physical accommodation for competing interests. Special procedural doctrines, such as the rule against prior restraint, are applied with some degree of firmness. All in all the print media are constitutionally well-entrenched.

The same does not apply, at least to the same degree, to the electronic media. There the physical scarcity of channels through which to communicate has led to greater government controls. Thus, despite the rule against prior restraint, no radio or television station can operate without first obtaining a license from the government. Some control over content is permitted. A broadcasting station must operate in "the public interest"; various limitations on ownership are imposed, such as prohibition against cross-ownership of newspapers and television stations; broadcasters must comply with the fairness doctrine and grant equal time to candidates for election. Furthermore, in the *Pacifica* case the Supreme Court upheld restrictions on the use of "offensive" language by broadcasting stations, resting its decision in part upon the special capacity of radio and television signals to enter the home.

One impact of the revolution in technology is a merging of the print and electronic modes of communication. Thus a facsimile newspaper may be sent into the home by electronic means. Access to information in a computer is in many ways similar to access to a library. The question has been raised as to whether, under these circumstances, the First Amendment law applicable to the print media or that applicable to the electronic media will be applied to the emerging modes of communication. In the former case government power over the media would be substantially more limited than in the latter case.

It is impossible to foresee how these matters will turn out. On the face of it, however, it would appear that the grounds for invoking First Amendment electronic law—the scarcity of physical facilities for communication—will largely disappear as a consequence of the new technology. If this be true, then First Amendment principles would certainly restrict governmental intervention in the system to matters of engineering and measures to limit monopoly.



Unless the *Pacifica* theory prevails, and electronic communication is held to possess a unique character, the result should be enhanced, not diminished, First Amendment rights.

The other feature of the modern technology is that it creates the physical facilities for virtually unlimited access to the means of communication. Thus, in place of the relatively few channels available for traditional television broadcasting, cable television allows a hundred programs to be broadcast simultaneously over a single wire. Whether this potential for expanding the volume and diversity of expression is realized in practice is one of the urgent open questions of the day. Increased exercise of First Amendment rights will not come about automatically. Positive steps to achieve that result will have to be taken. Thus, legal doctrines to govern the new situation will need to be formulated. For example, common carrier concepts, by which the instruments for communication can be available to all who pay a reasonable cost, have to be modernized. The actual measures necessary to assure that the new potential for expanded communication materializes fall within the province of the legislative and executive branches of government. The courts, however, retain the function of guiding and channeling these measures within the boundaries of the Constitution. The outcome of this process will in large measure determine how effectively the First Amendment will operate in the new technological world.

Affirmative Governmental Action Affecting First Amendment Rights

Most of our First Amendment law deals with the negative force of the First Amendment in preventing the government from prohibiting or interfering with freedom of expression. Yet some governmental conduct of a more affirmative nature may also have an impact upon First Amendment rights. Thus, the government may undertake to promote the system of freedom of expression by assisting speakers in their endeavors to communicate, or it may participate in the system itself as a speaker. Along with other governmental functions, these activities of the government have been increasing at an accelerated rate. Obviously, they both confer important benefits and present acute dangers.

First Amendment doctrine concerned with governmental conduct in this area is just beginning to develop. It is likely to become a critical issue for future generations. Some of the problems to be solved are illustrated by the use of government subsidies to finance various forms of expression and by government participation in expression through the operation of school libraries.

Government funding of expression takes place on a widespread scale. It includes giving financial support to public radio and television, providing public money for political candidates, making grants for scientific research, and furnishing financial aid to cultural activities. The principal First Amendment difficulty is that, in carrying out such programs, the government must designate the basic purposes for which public funds are to be made available and it thereby passes judgment on the content of the expression, preferring the subsidized to that not subsidized. Moreover, by the very nature of the relationship, the government is in a position to dictate or influence the message communicated by the beneficiary of the funds. The resolution of this dilemma would seem to rest in part upon developing a distinction between government intervention at the macro level and governmental intervention at the micro level. Thus, the government would be authorized to support expression by selecting a general area for subsidy but prevented from controlling the details of the expression within that area.

A different kind of issue is presented by the government's conduct in maintaining a school library. Questions arise when public officials remove or fail to provide a book because of its ideological content. A persuasive argument can be made that such action violates First Amendment rights. The function of the school, at least above the elementary level, is not only to instill

traditional knowledge in its students but to give them the capacity for critical thought and innovative action. The library is a key institution in this process. The student, who frequently is a captive audience because of the compulsory attendance laws, would appear to have a constitutional right to have access to a broad range of information and ideas. The Supreme Court in its recent decision in the *Island Trees School* case has indeed recognized such a right.

On the other hand, translation of the theoretical right into a concrete legal remedy is not without difficulty. In building a school library—adding or removing books—the school authorities must necessarily delve into the worth of the information and ideas contained in the material under consideration. By what standard is a court to decide whether this judgment violates the student's constitutional right? For answers the Court must look to concepts of balanced presentation and the professional judgment of educators as to whether the action of the school officials unduly restricts the space needed by the student for growth and development. Of course, even if the courts can formulate a workable standard they could not supervise every decision made by the school authorities. At most they would be able to keep the pertinent constitutional principles alive and apply them in egregious cases.

Affirmative government support of what is essentially a laissez-faire system and participation by the government in that system present a paradox. Government controls are brought into play, but the controls must in turn be controlled. The working out of this dilemma still remains a major task.

Conclusion

To sum up, there is some evidence that basic understanding and support for the system of freedom of expression have lost ground in some quarters. There are some weaknesses in the constitutional structure that has evolved from the decisions of the Supreme Court. The claims being pressed in the name of national security pose a critical issue; adjustment to the new technology demands an immediate solution; and controls over an active government, seeking to promote and participate in the system, have not yet evolved. Nevertheless, on the whole the First Amendment lives a powerful life. If we can keep basic economic, environmental, and other social conditions from overwhelming us, keep warfare from destroying us, and keep faith in the progress we have made, the symbolic year of 1984 need never arrive.

APPENDIX II

IV

98TH CONGRESS
1ST SESSION**H. RES. 384**

Expressing the sense of the House of Representatives regarding the blackout of press coverage in Grenada.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 18, 1983

Mr. LOWRY of Washington submitted the following resolution; which was referred to the Committee on the Judiciary

RESOLUTION

Expressing the sense of the House of Representatives regarding the blackout of press coverage in Grenada.

Whereas the first amendment of the Constitution of the United States provides that the freedom of the press shall not be abridged;

Whereas the United States Government has long been distinguished in the eyes of the world for its promotion and protection of press freedom and the open coverage and vigorous debate of issues and events;

Whereas the United States Government's protection of the freedom of the press has stood in stark contrast to the control of the press by the Government of the Soviet Union;

Whereas the American press corps has covered every military action involving the United States since the time of the American revolution;

Whereas hundreds of American correspondents have lost their lives covering American military activities around the world;

Whereas members of the press corps have consistently protected the secrecy of information which could jeopardize sensitive military operations or human lives;

Whereas the citizens in a democratic form of government rely on newspaper, magazine, television, and radio coverage of domestic and international activities of their government to develop informed and intelligent opinions about those activities; and

Whereas all members of the American press were uniformly prohibited by the United States Government from covering firsthand the American military intervention in Grenada:
Now, therefore, be it

- 1 *Resolved*, That it is the sense of the House of Repre-
- 2 sentatives that the President, executive officers, Congress,
- 3 and judiciary of the United States should honor and uphold
- 4 the protections of the press provided by the first amendment
- 5 of the Constitution of the United States and insure the right
- 6 of members of the press to bring to the American people
- 7 complete and uncensored reports of all future nonconfidential
- 8 military activities of the United States.

○



NEWS RELEASE

OFFICE OF ASSISTANT SECRETARY OF DEFENSE (PUBLIC AFFAIRS)
 WASHINGTON, D. C. 20301
 OFFICE OF THE SECRETARY OF DEFENSE

IMMEDIATE RELEASE

AUGUST 23, 1984

NO. 450-84

STATEMENT BY THE SECRETARY OF DEFENSE

I am today releasing the final report of the CJCS Media-Military Relations Panel (Sidle Panel).

I have directed the Assistant Secretary of Defense (Public Affairs) to take the necessary steps to implement those portions of the final report which meet the Panel's criteria of providing maximum news media coverage of U.S. military operations "consistent with military security and the safety of U.S. forces."

As an added step, I will form a panel of eminent journalists and former war correspondents to advise me on the best ways to meet these objectives. This group will become a permanent Secretary of Defense Media Advisory Committee. By forming such a committee, I wish to ensure that the media's viewpoint can be expressed in our highest councils on a continuing basis.

I firmly believe that relations between members of the armed forces and members of the press will be greatly enhanced by continued, strengthened, and informed dialogue. As part of instilling a better understanding on our part of the problems and responsibilities of the press in connection with our armed forces in times of crisis or conflict, as well as in peacetime, I have already directed a review of the adequacy of instruction on relations between the press and armed services at all levels of our military educational system.

I greatly appreciate the work done by General Sidle and the members of his panel, and by General Vessey. It is a necessary first step toward improved understanding by all parties. I believe our News Media Advisory Committee will help us move further and further along that path.

END

General John W. Vessey, Jr.
Chairman, Joint Chiefs of Staff
The Pentagon, Room 2E872
Washington, D.C. 20301

Dear General Vessey:

As you requested, enclosed are the final report and recommendations of the Sidle Panel, together with pertinent enclosures. The panel is unanimous in its strong belief that implementation of the recommendations, both in fact and in spirit, by the appropriate military authorities will set the stage for arriving at workable solutions for media-military relations in future military operations. We also believe that these solutions will be satisfactory to reasonable members of both the media and the military.

The report has three sections: an introduction, a recommendations section, and a comment section. We adopted this format because, while we were unanimous on the recommendations, there were some differences of opinion on some points in the comments. However, we all agreed that the comments were necessary to help explain the recommendations and that even the points on which we were not unanimous were worthy of consideration as suggestions and background for those who will implement the recommendations, should they be implemented. In any case, the entire panel has formally endorsed the recommendations, while I signed the comments. I should add that, where appropriate, I have mentioned the panel's degree of support in the comments.

The panel asked that I put three points in this letter that were not exactly germane to the report but required some comment on our part.

First, the matter of so-called First Amendment rights. This is an extremely gray area and the panel felt that it was a matter for the legal profession and the courts and that we were not qualified to provide a judgment. We felt justified in setting aside the issue, as we unanimously agreed at the outset that the U.S. media should cover U.S. military operations to the maximum degree possible consistent with mission security and the safety of U.S. forces.

Second, Grenada. We realize that Grenada had shown the need to review media-military relations in connection with military operations, but you did not request our assessment of media handling at Grenada and we will not provide it. However, we do feel that had our recommendations been "in place" and fully considered at the time of Grenada, there might have been no need to create our panel.

Finally, the matter of responsibility of the media. Although this is touched on in the report, and there is no doubt that the news organization representatives who appeared before us fully recognized their responsibilities, we feel we should state emphatically that reporters and editors alike must exercise responsibility in covering military operations. As one of the senior editors who appeared before us said, "The media must cover military operations comprehensively, intelligently, and objectively." The American people deserve news coverage of this quality and nothing less. It goes without saying, of course, that the military also has a concurrent responsibility, that of making it possible for the media to provide such coverage.

The members of the panel have also asked me to express their appreciation for being asked to participate in this important study and their hope that our work will be of value to the military, the media, and to the American people.

Finally, the panel considers this covering letter an integral part of our report.

Sincerely,



Winant Sidle
Major General, USA, Retired
Chairman

Enclosure
Report

INTRODUCTION

The Chairman of the Joint Chiefs of Staff (CJCS) Media - Military Relations Panel (known as the Sidle Panel) was created at the request of the Chairman, General John W. Vessey, Jr., who asked that I convene a panel of experts to make recommendations to him on, "How do we conduct military operations in a manner that safeguards the lives of our military and protects the security of the operation while keeping the American public informed through the media?"

Major General Winant Sidle, USA, Retired, was selected as chairman of this project and asked to assemble a panel composed of media representatives, public affairs elements of the four Military Services, the Office of the Assistant Secretary of Defense (Public Affairs) (OASD(PA)), and operations spokesmen from the Organization of the Joint Chiefs of Staff (OJCS).

The initial plan, concurred in by CJCS and ASD(PA), was to invite major umbrella media organizations and the Department of Defense organizations to provide members of this panel. The umbrella organizations, such as the American Newspaper Publishers Association (ANPA), the American Society of Newspaper Editors (ASNE), the National Association of Broadcasters (NAB), and the Radio Television News Directors Association (RTNDA), and their individual member news organizations decided that they would cooperate fully with the panel but would not provide members. The general reason given was that it was inappropriate for media members to serve on a government panel.

This decision, unanimous among the major news media organizations, resulted in a revised plan calling for the non-military membership of the panel to be composed of experienced retired media personnel and representatives of schools of journalism who were experts in military-media relations. The Department of Defense organizations involved agreed to provide members from the outset. Final panel membership is at Enclosure 1.

To provide initial input to the panel for use as a basis for discussion when the panel met, a questionnaire was devised with the concurrence of CJCS and ASD(PA) and mailed to all participants. It was also sent to a number of additional organizations and individuals who had expressed interest and to some who had not but were considered to be experts in the matter. As the result of these mailings, the panel had available 24 written inputs to study prior to meeting. Of these, 16 were from major news organizations or umbrella groups. All inputs are at Enclosure 2. The panel regretted that all who indicated interest could not appear before it, but time did not permit.

REPORT

by

CJCS MEDIA-MILITARY RELATIONS PANEL (SIDIE PANEL)

SECTION I: Recommendations

Statement of Principle

The American people must be informed about United States military operations and this information can best be provided through both the news media and the Government. Therefore, the panel believes it is essential that the U.S. news media cover U.S. military operations to the maximum degree possible consistent with mission security and the safety of U.S. forces.

This principle extends the major "Principle of Information" promulgated by the Secretary of Defense on 1 December 1983, which said:

"It is the policy of the Department of Defense to make available timely and accurate information so that the public, Congress, and members representing the press, radio and television may assess and understand the facts about national security and defense strategy. Requests for information from organizations and private citizens will be answered responsively and as rapidly as possible. . . ." (Copy at Enclosure 4)

It should be noted that the above statement is in consonance with similar policies publicly stated by most former secretaries of defense.

The panel's statement of principle is also generally consistent with the first two paragraphs contained in "A Statement of Principle on Press Access to Military Operations" issued on 10 January 1984 by 10 major news organizations (copy at Enclosure 5). These were:

"First, the highest civilian and military officers of the government should reaffirm the historic principle that American journalists, print and broadcast, with their professional equipment, should be present at U.S. military operations. And the news media should reaffirm their recognition of the importance of U.S. military mission security and troop safety. When essential, both groups can agree on coverage conditions which satisfy safety and security imperatives while, in keeping with the spirit of the First Amendment, permitting independent reporting to the citizens of our free and open society to whom our government is ultimately accountable.

"Second, the highest civilian and military officers of the U.S. government should reaffirm that military plans should include planning for press access, in keeping with past traditions. The expertise of government public affairs officers during the planning of recent Grenada military operations could have met the interests of both the military and the press, to everyone's benefit."

Application of the panel's principle should be adopted both in substance and in spirit. This will make it possible better to meet the needs of both the military and the media during future military operations. The following recommendations by the panel are designed to help make this happen. They are primarily general in nature in view of the almost endless number of variations in military operations that could occur. However, the panel believes that they provide the necessary flexibility and broad guidance to cover almost all situations.

RECOMMENDATION 1:

That public affairs planning for military operations be conducted concurrently with operational planning. This can be assured in the great majority of cases by implementing the following:

- a. Review all joint planning documents to assure that JCS guidance in public affairs matters is adequate.
- b. When sending implementing orders to Commanders in Chief in the field, direct CINC planners to include consideration of public information aspects.
- c. Inform the Assistant Secretary of Defense (Public Affairs) of an impending military operation at the earliest possible time. This information should appropriately come from the Secretary of Defense.
- d. Complete the plan, currently being studied, to include a public affairs planning cell in OJCS to help ensure adequate public affairs review of CINC plans.
- e. Insofar as possible and appropriate, institutionalize these steps in written guidance or policy.

RECOMMENDATION 2:

When it becomes apparent during military operational planning that news media pooling provides the only feasible means of furnishing the media with early access to an operation, planning should provide for the largest possible press pool that is practical and minimize the length of time the pool will be necessary before "full coverage" is feasible.

RECOMMENDATION 3:

That, in connection with the use of pools, the Joint Chiefs of Staff recommend to the Secretary of Defense that he study the matter of whether to use a pre-established and constantly updated accreditation or notification list of correspondents in case of a military operation for which a pool is required or the establishment of a news agency list for use in the same circumstances.

RECOMMENDATION 4:

That a basic tenet governing media access to military operations should be voluntary compliance by the media with security guidelines or ground rules established and issued by the military. These rules should be as few as possible and should be worked out during the planning process for each operation. Violations would mean exclusion of the correspondent(s) concerned from further coverage of the operation.

RECOMMENDATION 5:

Public Affairs planning for military operations should include sufficient equipment and qualified military personnel whose function is to assist correspondents in covering the operation adequately.

RECOMMENDATION 6:

Planners should carefully consider media communications requirements to assure the earliest feasible availability. However, these communications must not interfere with combat and combat support operations. If necessary and feasible, plans should include communications facilities dedicated to the news media.

RECOMMENDATION 7:

Planning factors should include provision for intra- and inter-theatre transportation support of the media.

RECOMMENDATION 8:

To improve media-military understanding and cooperation:

a. CJCS should recommend to the Secretary of Defense that a program be undertaken by ASD(PA) for top military public affairs representatives to meet with news organization leadership, to include meetings with individual news organizations, on a reasonably regular basis to discuss mutual problems, including relationships with the media during military operations and exercises. This program should begin as soon as possible.

b. Enlarge programs already underway to improve military understanding of the media via public affairs instruction in service schools, to include media participation when possible.

c. Seek improved media understanding of the military through more visits by commanders and line officers to news organizations.

d. CJCS should recommend that the Secretary of Defense host at an early date a working meeting with representatives of the broadcast news media to explore the special problems of ensuring military security when and if there is real-time or near real-time news media audiovisual coverage of a battlefield and, if special problems exist, how they can best be dealt with consistent with the basic principle set forth at the beginning of this section of the report.

The Panel members fully support the statement of principle and the supporting recommendations listed above and so indicate by their signatures below:

Winant Sidle
Winant Sidle, Major General, USA, Retired
Chairman

Brent Baker
Brent Baker, Captain, USN

Fred C. Lash
Fred C. Lash, Major, USMC

Keyes Beech
Keyes Beech

James Major
James Major, Captain, USN

Scott M. Cutlip
Scott M. Cutlip

Wendell S. Merick
Wendell S. Merick

John T. Halbert
John T. Halbert

Robert O'Brien
Robert O'Brien, Colonel, USAF
Deputy Assistant Secretary of Defense (Public Affairs)

Billy Hunt
Billy Hunt

Richard S. Sargent
Richard S. Sargent

George Kirschenbauer
George Kirschenbauer, Colonel, USA

Barry Loxton
Barry Loxton

R. P. Langguth
R. P. Langguth

SECTION II:

RECOMMENDATION 1:

That public affairs planning for military operations be conducted concurrently with operational planning. This can be assured in the great majority of cases by implementing the following:

- a. Review all joint planning documents to assure that JCS guidance in public affairs matters is adequate.
- b. When sending implementing orders to Commanders in Chief in the field, direct that the CINC planners include consideration of public information aspects.
- c. Inform the Assistant Secretary of Defense (Public Affairs) of an impending military operation at the earliest possible time. This information should appropriately come from the Secretary of Defense.
- d. Complete the plan, currently being studied, to include a public affairs planning cell in OJCS to help ensure adequate public affairs review of CINC plans.
- e. Insofar as possible and appropriate, institutionalize these steps in written guidance or policy.

Comments

1. Under the current system of planning for military operations, provisions exist to include public affairs planning but it is neither mandatory nor certain that current joint planning documents are adequate from a public affairs standpoint. The basic purpose of this recommendation is to help assure that public affairs aspects are considered as soon as possible in the planning cycle for any appropriate military operation and that the public affairs planning guidance is adequate.

2. The panel was unanimous in feeling that every step should be taken to ensure public affairs participation in planning and/or review at every appropriate level. Recommendations 1a, b, and d are designed to assist in implementing this consideration.

3. Panel discussions indicated that it is difficult to determine in advance in all cases when public affairs planning should be included. The panel felt that the best procedure would be to include such planning if there were even a remote chance it would be needed. For example, a strictly covert operation, such as the Son Tay raid in North Vietnam, still requires addressing public affairs considerations if only to be sure that after action coverage adequately fulfills the obligation to inform the American people. Very small, routine operations might be exceptions.

4. Recommendation 1c is self-explanatory. The ASD(PA), as the principal public affairs advisor to both the Secretary of Defense and the Chairman, JCS, must be brought into the planning process as soon as possible. In view of the DOD organization, the panel felt that this should be the responsibility of the Secretary of Defense.

5. We received indications that some commanders take the position that telling something to his public affairs officer is tantamount to telling it to the media. All members of the panel, including its public affairs officers decried this tendency and pointed out that a public affairs specialist is the least likely to release material prematurely to the media. Although the panel did not consider the matter officially, there is no doubt that public affairs officers are just as dedicated to maintaining military security as are operations officers and must know what is going on in a command if they are to do their job!

RECOMMENDATION 2:

When it becomes apparent during military operational planning that news media pooling provides the only feasible means of furnishing the media with early access to an operation, planning should support the largest possible press pool that is practical and minimize the length of time the pool will be necessary.

Comments

1. Media representatives appearing before the panel were unanimous in being opposed to pools in general. However, they all also agreed that they would cooperate in pooling agreements if that were necessary for them to obtain early access to an operation.

2. The media representatives generally felt that DOD should select the organizations to participate in pools, and the organizations should select the individual reporters. (See Recommendation 3.)

3. The media were unanimous in requesting that pools be terminated as soon as possible and "full coverage" allowed. "Full coverage" appeared to be a relative term, and some agreed that even this might be limited in cases where security, logistics, and the size of the operation created limitations that would not permit any and all bona fide reporters to cover an event. The panel felt that any limitations would have to be decided on a case-by-case basis but agreed that maximum possible coverage should be permitted.

4. The media agreed that prior notification of a pooling organization should be as close to H-Hour as possible to minimize the possibility of a story breaking too soon, especially if speculative stories about the operation should appear in media not in the pool or be initiated by one of their reporters not privy to the pool. This would require a pool media decision as to whether to break the story early, despite the embargo on such a break that is inherent in early notification for pooling purposes. The media representatives were not in agreement on this matter but did agree generally that they should not release aspects of the story that they had been made aware of during DOD early notification and which did not appear in the stories already out or in preparation; nor should this privy information be used to confirm speculation concerning an operation.

5. In this connection, the media generally did not agree with a view voiced by some members of the panel that, absolutely to guarantee security, pool notification would not be made until the first military personnel had hit the beach or airhead even though advance military preparation could speed the poolers to the site in the least time possible. The panel did not take a position on this, but some felt that carefully planned pool transportation could meet the media's objections in many, possibly most, cases. For example, in remote areas the pool could be assembled in a location close to the operation using overseas correspondent who would not have to travel from the United States. This is a subject worthy of detailed discussion in the military-media meetings proposed in Recommendation 8a.

6. In this connection, the panel recognized that in many areas of the world an established press presence would be encountered by U.S. forces irrespective of a decision as to whether or not a pool would be used. This consideration would have to be included in initial public affairs planning.

7. There was no unanimity among the media representatives as to whether correspondents, pooled or otherwise, should be in the "first wave" or any other precise point in the operation. All did agree that media presence should be as soon as possible and feasible. The panel believes that such timing has to be decided on a case-by-case basis.

8. Neither the media nor the panel agreed on use in a pool of full-time media employees who are not U.S. citizens. The media tended to agree that, if the parent organization considered such employees reliable, they should be allowed to be pool members. Based on public affairs experience in Vietnam, there were many cases where such employees proved entirely reliable; however, some did not. The panel suggests that this has to be another case-by-case situation.

9. There was also a divergence of opinion among the media as to what news organizations should make up a pool, although all agreed that the most important criterion was probably which organizations cover the widest American audience. Several media representatives suggested specific media pools, but, unfortunately, they varied widely. The panel was not in full agreement on this subject either, but did agree that the following types of news organizations should have top priority. The panel further agreed that DoD should take the factors discussed in this paragraph into account when designating news organizations to participate in a pool.

a. Wire services. AP and UPI to have priority. A reporter from each and a photographer from either one should be adequate. In a crash situation where inadequate planning time has been available, a reporter from one wire service and a photographer from the other could provide a two-person pool.

b. Television. A two-person TV pool (one correspondent, one film/sound man) can do the job for a brief time although perhaps minimally. All TV representatives agreed that a three-person team is better and can do more. A panel suggestion that a six-person team (one cameraman, one sound man, and one reporter each from ABC, CBS, NBC, and CNN) seemed agreeable to the four networks although the load on the two technicians would be difficult to handle. The panel has no suggestion on this except that TV pool representatives must have high priority with two representatives as the minimum and augmentation to depend on space available. This should be a matter of discussion at the meetings suggested in recommendation 8a. The question of radio participation in pools must also be resolved.

c. News Magazines. One reporter and one color photographer.

d. Daily newspapers. At least one reporter. The panel agreed with newspaper representatives that, although newspapers do use wire service copy and photos, at least one newspaper pooler is needed for the special aspects of newspaper coverage not provided by the wire services. Criteria suggested for use when deciding which newspaper(s) to include in a pool included: Circulation, whether the newspaper has a news service, does the newspaper specialize in military and foreign affairs, and does it cover the Pentagon regularly. There was some agreement among the media representatives that there are probably not more than 8-10 newspapers which should be considered for pooling under these criteria.

10. In addition to the type of embargo necessary when a pooling news agency is notified in advance about a military operation (i.e., nothing to be said about it until it begins) there is another type applicable to some military operations. This second type was used with great success in Vietnam and restricts media accompanying the forces from filing or releasing any information about the progress of the operation until the on-scene commander determines that such release will not impair his security by informing the opposing commander about his objectives. Normally, this is not a problem as general objectives quickly become apparent. In the case of a special objective, there might be some delay in authorizing stories until either the objective is attained or it is obvious the enemy commander knows what it is. In any case, this type of embargo is an option to planners that the media would almost certainly accept as opposed to not having correspondents with the forces from the outset or close to it. The panel did not have a consensus on this matter.

11. Media representatives emphasized the readiness of correspondents to accept, as in the past, the physical dangers inherent in military operations and agreed that the personal security of correspondents should not be a factor in planning media participation in military operations.

RECOMMENDATION 3:

In connection with the use of pools, the Joint Chiefs of Staff recommend to the Secretary of Defense that he study the matter of whether to use a pre-established and constantly updated accreditation or notification list of correspondents in case of a military operation for which a pool is required or just the establishment of a news agency list for use in the same circumstances.

Comments

1. The panel envisions that in either case the agency would select the individual(s) to be its representatives in the pool. In the case of the accreditation/notification list, there would presumably be several names from each news agency/organization to provide the necessary flexibility. The agency would have provided the names in advance to DoD. In the case of the news agency/organization list, DoD would decide which agencies would be in the pool and the agencies would pick the person(s) desired without reference to a list. There was no agreement as to whether DoD should have approval authority of the individuals named to be pool members. The media representatives were unanimously against such approval as were some members of the panel. However, other panel members believed that in the case of an extremely sensitive operation, DoD should have such authority.

2. There was no agreement among either those who appeared before the panel or among the panel itself on this matter. There in both groups seemed to favor simply establishing a news agency list including wire services, television, news magazines and newspapers from which to pick when DOD establishes a pool.

3. This particular problem is one that should be resolved in advance of a military operation and should be a subject of discussion in connection with the military-media meetings suggested in Recommendation 8a.

4. This recommendation does not concern the accreditation that would have to be given each correspondent covering an operation, either at first or later, by the senior on-site commander. Traditionally, this accreditation is limited to establishing that the individual is a bona fide reporter (represents an actual media organization).

RECOMMENDATION 4:

That a basic tenet governing media access to military operations should be voluntary compliance by the media with security guidelines or ground rules established and issued by the military. These rules should be as few as possible and should be worked out during the planning process for each operation. Violations would mean exclusion of the correspondent(s) concerned from further coverage of the operation.

Comments

1. The media were in support of this concept as opposed to formal censorship of any type, and all media representatives agreed that their organizations would abide by these ground rules. This arrangement would place a heavy responsibility on the news media to exercise care so as not to inadvertently jeopardize mission security or troop safety.

2. The guidelines/ground rules are envisioned to be similar to those used in Vietnam (a copy at Enclosure 6). Recognizing that each situation will be different, public affairs planners could use the Vietnam rules as a starting point, as they were worked out empirically during Vietnam by public affairs and security personnel and, for the most part, in cooperation with news media on the scene. All media representatives who addressed the issue agreed that the ground rules worked out satisfactorily in Vietnam.

RECOMMENDATION 5:

Public affairs planning for military operations should include sufficient equipment and qualified military personnel whose function is to assist correspondents in covering the operation adequately.

Comments

1. The military personnel referred to in this recommendation are normally called escorts; however, this term has developed some unfortunate connotations as far as the media are concerned. In any case, the panel's recommendation is designed to provide personnel who, acting as agents of the on-scene commander, will perform such functions as keep the correspondents abreast of the situation; arrange for interviews and briefings; arrange for their transportation to appropriate locations; ensure they are fed and housed, if necessary; and be as helpful as possible consistent with security and troop safety.

2. Almost all of the media representatives agreed that such escorts are desirable, especially at the beginning of an operation, to assist in media coverage. As the operation progresses and the reporters become familiar with what is going on, the media representatives were generally less enthusiastic about this type of assistance.

3. All the media were against escorts if their goal was to try to direct, censor, or slant coverage. However, most agreed that pointing out possible ground rule violations and security problems would be part of the escort's responsibility.

4. The point was made to the panel and the media representatives that escorts were often required in Vietnam, especially after about mid-1968, without many problems arising. One of the major advantages of escorts was making sure the reporters had a full and accurate understanding of the operation being covered.

5. The senior on-scene commander will decide how long escorting should continue after an operation begins.

RECOMMENDATION 6:

Planners should carefully consider media communications requirements to assure the earliest feasible availability. However, these communications must not interfere with combat and combat support operations. If necessary and feasible, plans should include communicative facilities dedicated to the news media.

Comments

1. Media representatives were unanimous in preferring provision for use of their own communications or using local civilian communications when possible. They were also unanimous, however, in the need for access to military communications if nothing else were available, especially in the opening stages of an operation.
2. Permitting media coverage without providing some sort of filing capability does not make sense unless an embargo is in force.
3. Although not discussed in depth during the panel meetings, communications availability is an obvious factor in determining press pool size. Planners should consider the varying deadlines of the different types of media. For example, newsmagazine reporters usually have more time to file thus permitting courier service as a possible satisfactory solution from their standpoint.
4. There was considerable discussion of the possibility of media-provided satellite uplinks being a future threat to security if technology permits real-time or near real-time copy and film/tape processing. The media representatives felt that such a possibility was not imminent; however, the discussions resulted in Recommendation 8d being included in the report. One panel member made the point that such real-time or near real-time capability has long existed for radio news including the Murrow reporting during World War II.

RECOMMENDATION 7:

Planning factors should include provision for intra- and inter-theater transportation support of the media. There was no Panel comment on this matter.

RECOMMENDATION 8:

To improve media-military understanding and cooperation:

- a. CJCS should recommend to the Secretary of Defense that a program be undertaken by ASD(PA) for top military public affairs representatives to meet with news organization leadership, to include meetings with individual news organizations, on a reasonably regular basis to discuss mutual problems, including relationships with the media during military operations and exercises. This program should begin as soon as possible.
- b. Enlarge programs already underway to improve military understanding of the media via public affairs instruction in service schools and colleges, to include media participation when possible.

c. Seek improved media understanding of the military through more visits by commanders and line officers to news organizations.

d. CJCS should recommend that the Secretary of Defense host at an early date a working meeting with representatives of the broadcast news media to explore the special problems of ensuring military security when and if there is real-time news media audiovisual coverage of a battlefield and, if special problems exist, how they can best be dealt with consistent with the basic principle set forth at the beginning of this section of the report.

Comments

1. The panel became convinced during its meetings with both media and military representatives that any current actual or perceived lack of mutual understanding and cooperation could be largely eliminated through the time-tested vehicle of having reasonable people sit down with reasonable people and discuss their problems. Although some of this has occurred from time to time through the years, there has not been enough, especially in recent years. The panel envisages that these meetings would be between ASD(PA) and/or his representatives and the senior leadership of both media umbrella organizations and individual major news organizations. A number of media representatives appearing before the panel said that they thought the media would be happy to participate such a program. The program should include use of the Chiefs/Directors of Public Affairs of the Services, some of whom are already doing this.

2. Such meetings would provide an excellent opportunity to discuss problems or potential problems involving future military operations/exercises such as pooling, security and troop safety, accreditation, logistic support, and most importantly, improving mutual respect, trust, and standing, and cooperation in general.

3. The panel does not exclude any news organizations in this recommendation, but practicality will lead to emphasis on meetings with major organizations. It would be equally useful for commanders in the field and their public affairs officers to conduct similar meetings with local and regional media in their areas, some of which are also underway at this time.

4. Both the panel and the media representatives lauded the efforts underway today to reinsert meaningful public affairs instruction in service schools and colleges. Many officers are sheltered from becoming involved with the news media until they are promoted to certain assignments where they suddenly come face-to-face with the media. If they have not been adequately informed in advance of the mutual

with each other, they sometimes tend to make inadequate decisions concerning media matters. In this connection, several media representatives told the panel they would be, and in some cases have already been, delighted to cooperate in this process by talking to classes and seminars.

5. Several media representatives also were enthusiastic about undertaking an effort to inform their employees about the military, primarily through visits of commanders and other appropriate personnel to their headquarters or elsewhere in their organizations. It was also apparent that some media are concerned with this problem to the point that they are taking an introspective look at their relations not only with the military but other institutions.

General Comments:

1. The panel agreed that public affairs planning for military operations involving allied forces should also consider making plans flexible enough to cover allied media participation, even in pools in some cases.

2. It was pointed out to the panel and should be noted that planners may also have to consider the desires of U.S. Ambassadors and their country teams when operations take place in friendly foreign countries. Some of these problems can, of course, be handled by the commanders and senior public affairs personnel on the scene, but they should be alerted to them in advance.

3. The media representatives all agreed that U.S. media should have first priority in covering U.S. military operations. The panel generally agreed that this must be handled on a case-by-case basis, especially when allied forces are involved.

Final Comment:

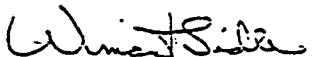
An adversarial -- perhaps politely critical would be a better term -- relationship between the media and the government, including the military, is healthy and helps guarantee that both institutions do a good job. However, this relationship must not become antagonistic -- an "us versus them" relationship. The appropriate media role in relation to the government has been summarized aptly as being neither that of a lap dog nor an attack dog but, rather, a watch dog. Mutual antagonism and distrust are not in the best interests of the media, the military, or the American people.

In the final analysis, no statement of principles, policies, or procedures, no matter how carefully crafted, can guarantee the desired results because they have to be carried out by people -- the people in the military and the people

in the media. So, it is the good will of the people involved, their spirit, their genuine efforts to do the job for the benefit of the United States, on which a civil and fruitful relationship hinges.

The panel believes that, if its recommendations are adopted, and the people involved are infused with the proper spirit, the twin imperatives of genuine mission security/troop safety on the one hand and a free flow of information to the American public on the other will be achieved.

In other words, the optimum solution to ensure proper media coverage of military operations will be to have the military -- represented by competent, professional public affairs personnel and commanders who understand media problems -- working with the media -- represented by competent, professional reporters and editors who understand military problems -- in a nonantagonistic atmosphere. The panel urges both institutions to adopt this philosophy and make it work.



Winant Sidle
Major General, USA, Retired
Chairman

Two Routes to the Wrong Destination: Public Affairs in the South Atlantic War

by

Lieutenant Commander Arthur A. Humphries, US Navy

The conflict in the South Atlantic in mid-1982 between Argentina and Great Britain offers us the opportunity to examine news management and its effects on public opinion in a crisis. This undeclared limited war for the Falkland Islands, or Malvinas, also provides us with a classic view of the differences in public information policies in an authoritarian government and in a democratic society. My intent is not to discuss the morality of propaganda, sophism, or blatant lying by a government in a crisis but to account for its existence and explain why and how it happens, along with the less oblique problems of misinformation and speculation.

There has been a tendency in the wake of the crisis to compare the public affairs or news aspects to America's experiences in the Vietnam conflict. I don't think that Vietnam provides an apt comparison. While both Vietnam and the Falklands were limited wars, there were too many dissimilarities to allow for historical analogy, especially in the area of public information. There was a great deal of time for the US Military Assistance Command in Vietnam and the government back home to plan and set up facilities for the press corps in Vietnam. The news media also had a great deal of time to develop attitudes about, and strategies for, approaching that particular crisis. There was no such urgency in Vietnam as we saw in the South Atlantic. But there was one striking similarity—the capability for immediate mass communication.

Mass Communications. There was the potential in the South Atlantic to show the folks back home a vivid, real-life, real-time picture of men from two opposing nations on two ordinary and theretofore unimportant islands doing some very permanent, ugly things to each other. After the Vietnam Tet Offensive of 1968, the American public, and for that matter the whole world, saw a sample of South Vietnamese-style capital punishment—a real execution of an enemy soldier, via their television sets in their own homes. That is not the sort of thing that would engender support at home for a war. If you want to maintain popular support for a war, your side must not be seen as

ruthless barbarians. Realistically, you cannot expect them always to be portrayed as knights in shining armor, either.

When relatives of servicemen see their boy, or someone who could be their boy, wounded or maimed, in living color, through imagery right in front of them, that tends to erode their support for their government's war aims. That happened during the Vietnam war. We know what happened to public opinion as a result of repeated doses of blood and guts given to a public that wasn't prepared to cope with it. The issue remains, then: What can a government do about that sort of problem, given the factors of high-tech communications capabilities and a worldwide public attuned to freedom of information?

The Public Affairs Problem. Public opinion was vital to the initiation and the conduct of the South Atlantic war. Except in a totalitarian state a war cannot be conducted without first mobilizing the public; but there are certain public affairs strategies and tactics which can work and others that are not likely to work in the process of mobilizing and exploiting public support for a war. What were the strategies and tactics used by the belligerents in this conflict to achieve and maintain public support? Were they effective? How were those strategies facilitated? As the primary media for the belligerent governments' messages, what were the reactions of the print and electronic news organizations to those strategies and tactics? What wisdom is gained about the ways of mobilizing and exploiting public support for a war in a modern industrial democracy?

Wisdom Relearned. The public affairs wisdom gained from the Falklands war certainly wouldn't be considered conventional wisdom, that is, in a society accustomed to free information. The unconventional wisdom might play badly in such news and mass communication jungles as Rockefeller Center in New York or Fleet Street in London. The unconventional wisdom plays well, however, in Buenos Aires; there is little or no choice but to accept it there. Yet, in spite of a perception of choice in a democratic society, the Falklands war shows us how to make certain that government policy is not undermined by the way a war is reported.

Here's the wisdom: control access to the fighting, invoke censorship, and rally aid in the form of patriotism at home and in the battle zone. Both Argentina and Great Britain showed us how to make that wisdom work. One of Britain's correspondents from World War II, the father of Falklands war correspondent Max Hastings, made the point then and it can still apply: "Objectivity can come back into fashion when the shooting is over." And, when the war was over, the armchair PAO quarterbacks could reflect with some objectivity that the disinformation from the British government and military was intended to deceive the Argentines; whereas the disinformation from the Argentine junta was intended to deceive the Argentine public.

Road to War. The Argentines had a public information plan and a psychological action plan for this war. Both plans are still classified and are still inaccessible. The British, on the other hand, winged their public affairs efforts. Except for the British Official Secrets Act, facilitated by a D-Notice Committee, there were no official British public affairs guidelines or directives to help the news management efforts of this war at the outset. There was a PAO plan on the shelves, a draft originated by the army in 1977, but it was discovered far too late to be of any help, at least for this war. It's not surprising that the MOD didn't have public affairs plans, knowing as we do now that they didn't have operational plans for anything outside of a Nato context.

The Argentines were prepared and so ever increasingly confident of their position that they even announced publicly their imminent invasion. On 24 January 1982, General Galtieri promised in a *La Prensa* article to possess the Malvinas before 3 January 1983, before the British and Falklanders could celebrate the 150th anniversary of the British settlement. Even certain members of the Argentine Embassy in the United States held no reservations, over cocktails or private dinner parties, about early advertisement of their government's intentions.

One month later, on the 24th of February, the British press warned of suspicious Argentine movements. Had the British become so complacent that they could mark these forthright warnings as only dictatorial rhetoric? It certainly seems that senior Foreign Office and MOD officials were satisfied with that explanation though they could read otherwise in their daily newspapers and in similar warnings from their embassy in Argentina. The British government made a fateful decision. At every turn they simply seemed to say to Argentina, "Come ahead and have your pleasure. We're not really interested in coming to a conclusion on our negotiations for the islands; we're not interested in defending them either since we're getting ready to scrap our only vessel there, the *Endurance*, plus some of our amphibs here, and we're selling our ASW carrier *Invincible* to Australia." With that kind of response to their warnings, the Argentines felt pretty comfortable about recouping what they saw as rightfully theirs.

So it was with that set of preliminaries that the Argentine occupation of the Falkland Islands took the British public by surprise. Yet, in spite of Britain's perceived indifference indicated to Argentina, the Falkland invasion was seen by the British public as an affront to British sovereignty and national pride that could not be ignored.

The British Performance

Prime Minister Thatcher had stronger public opinion behind her than any of her predecessors facing an international crisis, except Churchill, who in 1940 rallied his public in their country's greatest danger. A

large majority of Parliament, most of the public, and the news organizations enthusiastically supported their government's determination to use force if a settlement couldn't be negotiated. A public opinion poll showed 83 percent in favor of regaining the Falklands and 53 percent preferred the use of force. The latter percentage was to increase as negotiations faltered. *The Times* of London had a clear vision of what was necessary when, on 8 April it editorialized that: "In strategy one must disregard the method by which the decision is reached and consider only the outcome that is desired. That outcome is to force our adversary to accept certain terms which must be imposed on him and which, at present, he says are unacceptable. In the dialectic of wills the decision can be achieved not just through a clash of arms but psychologically"

The day before, another British daily, *The Guardian*, said, ". . . we must be sure that British opinion is prepared—through the waves of fervour—for a solution that meets the needs of the Falklanders." These editorial comments thus reflected the majority and indicated, at least here in postmortem, a willingness by these news organizations to do their part to win the war. Could the MOD afford to look so closely in the mouth of this seeming gift horse?

Good Policy, Bad Technique. Margaret Thatcher rose to her country's crisis openly and with honest explanation to her constituents. She bore the Parliamentary brunt of hard questions about lack of advance warning or preparation. She did not deceive or manipulate. It was she who insisted that to allow only six journalists to embark with her Falklands fleet was not enough. More had to be allowed to go. In the end, 29 journalists, technicians, and photographers sailed with the fleet. Her principle was right—allow coverage of the British side of the war. Her initiation of that principle was right—send journalists to tell the story. It was the inadequacy and the lack of a technique in managing the journalists, that harmed her government's public information effort.

Two principles—the public's right to information and the duty to withhold information for operational security—were the government's basis for information policy. They are not, nor do they have to be, diametrically opposite, in theory at least. But in actual practice they can easily conflict. The concept of operational security can be justified too loosely with such a response as, "that's an operational matter," particularly if the information being referred to is uncomplimentary to the person or unit or circumstance being discussed. If that happens, then the news media, writing for public consumption, will lose confidence and respect for the government or military spokesmen reflecting that attitude.

The other consideration, however, is the possibility of the news media becoming too cavalier with sensitive information because of naiveté,

"What I have said throughout to that kind of question is that interesting though it may be, I have throughout the whole of the last four weeks never made a comment on it, but have always said that I hope that no one will think my comment means more than, quite simply, no comment."

**British MOD Spokesman
Ian MacDonald
Falklands War briefing**

pressures of deadlines, self-righteousness, or political bias. At that point a government might lose any willingness to release even nonsensitive information. Where exactly the balance could be found, came out in Parliamentary investigation as one of the major difficulties involved in formulating information policy. There is some wisdom to be gained from the dilemma. It is vital that no government seeks, in its urgent need to prosecute a war successfully, to insulate itself from the process of public accountability.

What then should be reported by a government in war? The basic aims of an information policy should be: to provide as full an account as possible of the course of the conflict that is consistent with operational security; to retain the credibility of the government's or military's spokesmen; and to explain the government's case at home and to the international public. In the early stages of the Falklands war, the emphasis was on diplomatic activity, with the military preparations as part of the psychological pressure to achieve diplomatic settlement. At this point it was important for the government to show the resolve and capacity to win militarily, if necessary. When diplomacy failed and fighting started, the aim had to be to release information as quickly and as accurately as possible consistent with the safety and security of the task force.

Was it the MOD's policy always to tell the truth or did they indulge in misinformation in order to deceive the enemy? MOD representatives have freely admitted, and without apology, that they did not always tell the whole truth. They were unwilling though to admit that, on occasion, they deliberately misled the news media in order to deceive the Argentines.

The Ministry of Defence public information policy for this war, according to its Permanent Undersecretary, Sir Frank Cooper, was based on the assumption that "the public has both an interest in and a right to know about defence. But we do not regard these rights as unlimited."

Force commanders were specifically instructed "not to interfere with the style and content of press copy other than on security grounds," while news editors back home were "exceptionally cooperative" in responding to requests from MOD public relations personnel to remove certain references in stories in order to safeguard morale or to minimize distress to next of kin. Whether such an arrangement would be sufficient in a war in which

"instant" television coverage was possible, or in which the scope of the operation was more general, is dubious. What is a commander or a public affairs officer to do about it?

One journalist testifying before a Parliamentary investigating committee noted in this regard that he did not know of any British correspondent who had ever slanted a battle report or knowingly put troops' lives at risk. But, the journalist added, Mao Zedong was only 75 percent right when he said, "Power comes from the barrel of a gun." In an age of near-instant communication, power also bounces down a beam from a communications satellite and goes to the side which tells the story first. The Israelis are masters at this. While they use strict censorship, their military press officers are not usually obstructive and have the sense to make sure that reporters' copy gets out with all possible speed and that correspondents are given every possible assistance in the field. To a lesser degree, even rag-clad guerrillas are aware of the power of communication.

It was in that censorship or vetting process that the British gained some experience from which we can learn. During the Falklands war, there appeared to be no clear guidelines for censoring or vetting news reports. What the "minders" or censors with the task force and in London did, was something in between censoring and vetting, in that they appraised the correspondents' copy and asked them to remove or rewrite certain passages. The trouble was they didn't do it within a consistent format. Some of it was even ludicrous. As an example, in the pooled copy after the *Sir Galahad* was hit, there was a reference to a young guardsman, 20-year-old Stephen Dobbin. The reporter quoted him as saying, minutes after the attack, "Just tell my mum I'm safe, and keep your chin up. We'll get the bastards next time." The details of Guardsman Dobbin were bracketed by an MOD censor in London, who pointed out in brackets at the end of the dispatch: [The next of kin of Stephen Dobbin have not yet been informed, therefore we would appreciate his name not being mentioned.]

With the heavy-handedness of Sir Frank's organization in censoring journalistic and photographic products from the fleet, and the force commanders' difficulty in managing the news correspondents in their efforts, it is not surprising that not a single picture was taken of the Argentine surrender. Few people at the Ministry of Defence seemed to appreciate that news management is more than just information security censorship. It also means providing pictures.

The British Commander of the Land Forces, Major General Jeremy Moore, explained that he was being cautious with the negotiation process because of the uncertainty of the situation. The Argentine commander of the Falklands, General Mario Menendez, he explained, was not getting a clear agreement from his government to surrender on behalf of all Argentine forces. Moore added that, in his opinion, it would have been unsafe to allow

any possible distraction to endanger the agreement to surrender. In fact, two military photographers were in the building where the negotiations took place, waiting for the opportunity to document the surrender visually. But, in light of his guidance from London, the approach to publicity adopted by Moore was to secure the surrender as the highest priority and so avoid further loss of life. It is certainly conceivable that Menendez asked Moore not to allow photography of the negotiations or of the instrument signing. It is obvious that the omission of photographers was a deliberate move by Moore rather than an oversight. The point is that Britain was caught in another Argentine psychological ploy, as Argentina still argues to this day that they did not capitulate. Where the general public might not understand the subtle nuances of statesmanship, they certainly understand a simple picture.

On the day the *Sheffield* was fatally hit by an Argentine air-launched Exocet missile, the embarked journalists were told that the story had been embargoed by CinC Fleet in England. Similarly, the story of two Harriers colliding in fog was held up by the civilian censors with the task force, but the details of these and other similar incidents were released in London—causing a great deal of frustration for the reporters at sea. Their concern was not so much that their copy was being vetted for security purposes but that it was not getting to their home offices on time, if at all, and that the apparent lack of coordination between PAO personnel at sea and in London would keep these writers from their mutually agreed upon and appointed task.

So there was a serious information problem with the MOD. It arose not through any Machiavellian desire to mislead the news media or the public constantly, but through sheer incompetence at times and most often through naiveté.

One must say—in defense of the PAO effort at sea, for instance—that, although it was not possible to respond to all of the demands of the journalists, during the course of the operation over 600 dispatches and 50 hours of broadcasting tapes were sent back home by the embarked correspondents. Written copy alone amounted to over half a million words. The five reporters in the *Invincible* alone provided between 25 and 30 percent of the daily workload for the ship's communications center. At one stage it had a backlog of over 1,000 messages for transmission, but the *Invincible* correspondents were still able to send over 4,000 words of copy a day.

News Media Reaction. The government and MOD fared pretty well in spite of themselves. The conservative press was uniformly supportive of the government throughout the war. Much of the independent press also generally supported the government, in spite of hard warnings to the Prime Minister to pursue every effort to secure a negotiated settlement and continued warnings of the costs of military action. Even the liberal press was surprisingly supportive of the need to back up negotiations with a show of force.

There are charges and countercharges of censorship and irresponsibility, jingoism and bias. The evidence reinforces many of the popular prejudices of both the military and the news media about each other, particularly in times of stress. For the most part, the news representatives felt that the Ministry of Defence had a terrible war as far as public information management was concerned. However, there were some who would disagree. They are the ones who made the best of a tough situation and were able to write good stories and get them home.

The British news people reporting this war, whether at sea or in England, were, for the most part, generally unhappy with the arrangements made by the MOD for information matters. Specific complaints ranged from the inadequacy of the number of places for journalists to accompany the task force and the allocation of those places that were available, to the inconsistent censoring procedures used and the irregularity of briefings in London about the progress of the campaign. It was also argued that the lack of briefings contributed to the flood of speculative stories in the news. The first points can be chalked off to lack of planning by both parties, and frequently to a juvenile attitude by reporters, publishers, and TV executives who are too often used to getting their way. But the latter point, regarding briefings, deserves some more discussion because it is a problem at sea and ashore, and is an everyday problem, or consideration, for those who need or want to explain their story.

One of the most obviously mistaken decisions of the Ministry of Defence was to cease background briefings between the time of departure of the task force and 11 May by which time the naval campaign was well along. It is essential that a government and its military branch give regular briefings to representatives of all news organizations, as practicable, in order to sustain a relationship of trust, to foster the flow of correct information, and to halt faulty speculation. That is basic and essential to the success of any public affairs activity.

Reporters and their bosses do not like to think of themselves, or be thought of, as simply mouthpieces of government, or any other organization for that matter, except on their editorial pages. Most of them believe that their main responsibility is to provide the public with as complete and accurate an account as possible of any conflict in both its military and political aspects. In order to do that, they take advantage of all possible sources of information, official and unofficial, from home and overseas. News organizations are also very competitive and that creates a demand for dramatic and immediate news, which can interfere with the requirements of balance and impartiality, as well as those of completeness and accuracy.

When the MOD wouldn't provide the information, it is not surprising then, that television and the papers began using retired military officers to help them report what was probably going on in the Falklands. Nor is it

64 Naval War College Review

surprising that, during the first half of the war, British media were reporting information supplied by the Argentines. The problem is, most news organizations are businesses, and without capital in-flow, they cease to exist. So it is their goal to maintain and nurture their audience or readership. In order to do that, they must have a story—a story that beats their competition. If a government, or a military organization, or any group for that matter, understands that line, then they will know why it is vital to tell their story first, before their competition or enemy tells his.

Reaction in the MOD. In a democracy where everybody may have his say, there are bound to be dissenting voices. Dissent did not dissipate the national will during Britain's fight to regain the Falkland Islands; but it was a war won without consistent, even-handed, professional information services of the Ministry of Defence. The evidence I've seen indicates overwhelmingly that the lack of an experienced professional public relations officer at the head of the MOD public relations chain was widely felt in the news management of this war. This crisis made it abundantly clear that the Royal Navy and the British MOD need a public affairs plan for contingencies or for anything other than routine operations. Since the war the MOD has contracted with University College Cardiff to review the public relations problems of the Falklands war and develop a plan for them. It would be foolish for plans, which incorporate the news media into the organization for war, to be too firmly tied to a particular environment, but it is clear that information matters are an intrinsic part of war and should, therefore, form part of the planning for war.

The Falklands war drove the point home to military seniors that a far greater understanding of the nature of news work is necessary within the armed services. News media studies should form an integral part of higher defense training. To that end, the incorporation of a public affairs element in exercises would be of great value to the military, particularly the Royal Navy, and the news media.

The Ministry of Defence believed they had "got it about right" and were generally pleased with the outcome. That's the official line. Unofficially, the attitude is that they were very unhappy about having had to take so many journalists to sea, embarrassed about their own lack of planning and inability to manage the press, and displeased with the low priority the press was given in the operation—particularly as regards communications, transportation, and other simple logistics.

Perhaps the military commanders' most noteworthy objection to the flow of information to the public was over the release too soon or of too much operational information that could jeopardize both the lives of fighting men and the success of their efforts. It also bothered the relatives and friends of those sailors, marines, and soldiers who were fighting for the Falklands. The

Parachute Regiment was incensed over a premature BBC report which said they were attacking Goose Green, an attack that, when it took place shortly afterwards, cost many lives including the battalion commander's. But that was a fault of the government in releasing the information, not of the broadcaster who took its release at face value. One flag officer said that the Navy's biggest concern in this regard was the reports released back home that Argentine air-dropped bombs were not exploding on impact with the British ships. Though the problem of publicizing operational information was discussed with London, he said it wasn't corrected.

While the task force commanders had absolute control of the mechanics of the information flow from the South Atlantic, they had no control and little, if any, influence over the information flow back home. Probably never again will the Ministry of Defence, or the defense department of any other democratic nation, be able to control all means of transportation to the scene of fighting and the sole means of communications both for copy and pictures. Knowing that makes it all the more important that plans should include criteria for incorporating the news media into the organization for war. It would be prudent to base those plans on principles agreed to by both parties—the news media and the military—taking into account the variety of operational circumstances which might arise.

If the presence of the news media in a crisis or a war is accepted as inevitable, one consequence must be to inform those media about the facilities that will and will not, be available to them. The frustrations the correspondents suffered in their efforts to report this war were occasionally directed at the military men they worked with, whose highest priority and principal efforts were directed toward the successful prosecution of the war and who were often neglectful of the needs of the news correspondents. And so it will be in any conflict that the operators have their jobs to do, and with a narrow focus, see the news media as an obstruction. The wider focus, however, must never be forgotten, that the news media can be a useful tool, or even a weapon, in prosecuting a war psychologically, so that the operators don't have to use their more severe weapons.

In its concluding remarks, the House of Commons Defence Committee investigating information problems in this war, summed up the problem nicely. That report says operational commanders must have a determination to win, but those concerned with the higher direction of operations need a wider grasp of the political and psychological elements of national security policy. Pursuit of short-term military advantage without regard to world opinion could be fatal militarily, as well as politically.

The Argentine Performance

In Buenos Aires the problems of public information were handled somewhat differently than they were in London. The Argentine joint

staff (Estado Mayor Conjunto) had the exclusive responsibility for releasing information about the war to the news media. In some cases the joint staff tried to apply objectivity; however, in most of their official communiques it is clear that their intention was to influence public opinion. The junta, through the joint staff, used misinformation to the point of sophism, or disinformation.

Voices of Government. The joint staff had its press releases organized in accordance with a still classified plan, according to a ranking governmental source in Argentina. Though the plan was designed to avoid any releases from nonofficial or nonjoint staff sources, spokesmen who were frequently perceived by the public to be officially sanctioned, committed gross acts of speculation and disinformation. These perceived government spokesmen were on the periphery of the junta in the form of unattributed "military sources." Most often they were government-owned and operated TV stations or government-influenced publications, which often profess government policies. The local publications sometimes created their own stories as if they were trying to outdo the government. An American television news producer who was in Argentina for the duration of the war described, in a recent interview with me, the reality of news organizations operating under an authoritarian regime. "It was remarkable for some of us who were a bit naive about how government-run media in other parts of the world can be part of the same ball game. It's as if they're out there with the flags in the first row, screaming and yelling the lies as much as anybody else would. And that's why they're there. That's how you become an editor or publisher of a big important newspaper or magazine in Argentina. It is because you know the party line better than the people who are the party."

Reporters for Argentina's leading publications regularly complained to their foreign peers during the war that their publishers told them how to orient their stories politically. During the war, *Gente*, a leading glossy weekly, ran a two-page interview with an Argentine commando allegedly contacted by radio behind the British lines on South Georgia Island. It was designed to spark public ardor for the war and for the boys at the front. As it turned out, the article was completely fabricated at the order of an editor.

Even though that sort of incident was not directed by the junta, it certainly worked nicely into their psychological efforts. Psychological action was one of the principles guiding the junta's domestic affairs. They started by preparing their public for war, not negotiations, and not just any war but a short one. The Argentine public affairs objectives were to whip up patriotic fervor for the war, to push for Latin American solidarity, and to show that Britain was the aggressor and Argentina the victim. Additionally, an Argentine government source says that yet another aim was to attempt to reduce animosity against the United States. It has been difficult to find evidence of that during the war.

Managing the Information. Unofficial sources of information were not the only origins of disinformation. One only need look at the official joint staff communiques to see an amazing level of sophism. While reportage and communique analysis is the subject of another detailed study, it is clear that the Argentines repeatedly understated their losses and overstated the damage inflicted on the British.

Some experts on Argentina might say that was the result of bureaucratic mistakes indicative of the regime there. A neophyte might not excuse a government for such repeated misstatements and simply call it lying. What I can say for sure is that before the end of May, the Argentine joint staff had claimed that their forces shot down more Harriers than the British owned. Moreover, if we are to believe central and peripheral Argentine government sources, the HMS *Invincible* was sunk five times during the war. Unfortunately, I could find no record of the Argentine public's response at the time to those misstatements. In spite of these examples and the Argentine public's negative postwar response to the junta's triumphalism, the joint staff claims that their public affairs and psychological action plans "worked fine, with some exceptions and lack of control."

Between 2 April and 21 June the joint staff released 170 communiques, a rate of more than two per day, regarding the government's policies and the situation in the battle zone. One communique assured the public that the information coming in to the staff for release would be "evaluated in volume as well as content to avoid inaccuracies and the creation of false expectations." If no information was released, according to their policy, then the public should rest assured that there was no important news to announce. Nonetheless there was a constant stream of information available from the Argentine side, particularly between the time of their invasion on 2 April, and the British buildup to the San Carlos landing on 21 May. There is no doubt that the speed with which Argentina released information was at times embarrassing to the British government. These embarrassments have been described by the BBC director, for example, as "a self inflicted wound."

The publicized governmental policy that guided news organizations reporting from Buenos Aires during this war was self-censorship, "so that press censorship and other restrictions would not be necessary." If there was a chance that reports "could damage the morale of the nation, then they should be avoided." The guidance to journalists said that "news agencies and/or correspondents accredited in the country will be responsible for the control of all information that originates in the country or coming from abroad which is transmitted or retransmitted either abroad or to national correspondents." Is this a policy we should admire? A recent Louis Harris poll shows that nine out of ten Americans feel that news media in this country should follow that policy, although the poll was not taken in the context of the subject of Argentina or the Falklands war.

In addressing the problem of national security, the Argentine joint staff guidelines prohibited information that would "produce panic, is against national unity, detracts from the credibility of, or contradicts official information, upsets internal order, generates aggressive attitudes toward the country's British community, affects the relationship with other countries, or coming from abroad, tends to facilitate the achievement of the opponent's psychological goals."

Regardless of that stiff policy for news correspondents, the point should not be overlooked that, indeed, the Argentine junta allowed British correspondents to stay on in Buenos Aires. And as one might expect of a democratic nation, Great Britain had no aversion to allowing Argentine correspondents to continue their work in England. It is worth recalling, however, speaking of democratic societies, that the United States was not as open-minded about Japanese correspondents between 1942 and 1945.

The Argentines did not have the infrastructure necessary to conduct formal censorship as the British tried to do. What they tried to do with the foreign press was what reportedly they do ordinarily with their own news media. That situation has been described by correspondents who were in Argentina during the war as a veiled semicensorship, backed up with at least harassment, if not violence. The possibility of government dissatisfaction and retaliation was not lost on the approximately 700 foreign correspondents reporting the war from Buenos Aires. An American TV news producer stationed in Buenos Aires for the war admitted that all the news organizations there "were virtually mouthpieces (for the government) in many cases. Our coverage was a bit contrived and a bit controlled." He added that the government effectively sent a message that "you'd better watch yourself, you'd better watch the kind of stories you're doing, you'd better watch who you intimidate and who you are going to insult, because we're very sensitive."

Is it the proper role of the press to intimidate or to insult? Many newsmen would say yes, if it is necessary to put a news subject off-balance in order that he might provide more information. My personal and professional attitude as a potential interviewee is that, I wouldn't stand for it and don't think any news interviewee should have to.

The Road to War. The task of preparing the Argentine public for a Malvinas invasion began late in December 1981, according to correspondents from *The Times* of London in their book *War in the Falklands*. That was after the takeover by the new president, General Leopoldo Galtieri. His foreign secretary, Nicanor Costa Mendez, met with a select group of Argentine journalists and discussed the government's intentions. According to *The Times* writers, Galtieri was determined to regain the Falklands—by diplomacy if possible, by force if necessary. Several weeks later, Argentina's premier newspaper,

La Prensa, printed a column that addressed the problem of the defense of the South Atlantic and said that taking the Malvinas by force was an option "which would enjoy an international consensus." A week later the same columnist who, it may be surmised, was speaking for his government, added in this regard that "the United States . . . would support all acts leading to restitution (of the Malvinas), including military ones . . ." That kind of public preparation for this war continued until the invasion on 2 April 1982.

Triumphalism. The view the Argentine government gave to its citizens and the world from the time of the invasion until the last days of this short war was reflective of its psychological action plan. It was a view of extreme triumphalism, even though the joint staff said that they were trying to avoid that. Starting with the approach of the British task force, through at least the Bluff Cove engagement in June, the Argentines were saying that their forces were invincible and the British would be sent home with a bloody nose. The vast majority of the Argentine public felt that their case was right and just and therefore were predisposed to accept a lot of the triumphalism.

During the course of the war, the Argentine public was perhaps more predisposed to believe the triumphalism espoused by the junta than they would have been to support the triumphalism of, say, a given economic or agricultural policy. Nothing can take the people's minds off a collapsing economy like a popular war. When the Ministry of Economy says the rate of inflation will be kept down to 100 percent this year and the people know it is going to be at least 300 percent, they make their own judgment on the ministry's information. The public was ready for a national victory of sorts, something upbeat for a change, having struggled with a brutally inflated economy for so long. So, when they kept hearing reports of their military forces triumphant in battle, they believed them, besides the general feeling that their case in the Malvinas crisis was right. But after the war, and here is a key point, there was a widespread revulsion and questioning of the triumphalism that was peddled by the junta via the Argentine press. The Argentines are understandably cynical and disillusioned. What little faith they had in the nation's institutions dissipated when, at the end of the war, they learned that they had been deceived by the military and the news media into thinking they were winning. A national television news show that bills itself as "The Hour of Truth" is now popularly called "The Hour of Lies."

Argentina's handling of war news demonstrates that lying to your people costs more in the long run than it gains in the short run. The country was bound up in a state of, as the *Christian Science Monitor* put it, national self-deception. A hungry public was quick to swallow the junta's triumphalism. The misstatements of war information were readily believed when the public read them as official communiques from the joint staff. Conversely, when anything was going badly for the Argentines, the British reports to the

contrary were laughed off as propaganda or psychological warfare. It is not surprising, then, that the public and many in the military were at first stunned when news came of the British landings. The public and many members of the armed forces thought they were winning until the last moment when they lost. The Argentine psychological action plan would not even allow reports of the 250 dead at Goose Green and 1,400 taken prisoner, even as the British troops were taking Port Stanley.

While there is no credit due the Galtieri junta for trusting its public with good and bad news of the war, the Thatcher government can be accused of the same shortcoming. But, as can be seen from the experience of the Galtieri regime, the government that blatantly lies to its people cannot ultimately endure. Thus we can end this chapter with a bit of morality and philosophy from Sissela Bok: "The language of enmity and rivalry is not suited to moral inquiry. If we want to produce excuses for lying to someone, these excuses should be capable of persuading reasonable persons, not merely some particular public locked in hostility to a particular group. Entering into hostilities is, in a sense, to give up the ability to shift perspectives. But even those who give up the language of morality during a period of hostility and adopt that of strategy instead, may do well to remember Mark Twain's words: 'When in doubt, tell the truth. It will confound your enemies and astound your friends.'"⁶

A Better Route, A Better Destination

The conflict in the South Atlantic in mid-1982 between Argentina and Great Britain offers us the opportunity to examine news management and its effects on public opinion in a crisis situation.

Some of the conclusions I've developed as a result of this study of the public affairs aspects of the Falklands war are:

- To maintain popular support for a war, your side must not be seen as ruthless barbarians;
- If you don't want to erode the public's confidence in the government's war aims, then you cannot allow that public's sons to be wounded or maimed right in front of them via their TV sets at home;
- You must, therefore, control correspondents' access to the fighting;
- You must invoke censorship in order to halt aid to both the known and the suspected enemies;
- You must rally aid in the form of patriotism at home and in the battle zone but not to the extent of repeated triumphalism;
- You must tell your side of the story first, at least for psychological advantage, causing the enemy to play catch-up politically, with resultant strategic effect;
- To generate aid, and confuse at least the domestic detractors, report the

⁶*Lying—A Moral Choice in Public and Private Life* (New York: Pantheon, 1978), p. 145

truth about the enemy and let the enemy defectors tell their horror story.

- Finally, in order to affect or help assure "favorable objectivity," you must be able to exclude certain correspondents from the battle zone.

Now that the first South Atlantic crisis of the century has been through "Hot Washup," the PAO armchair quarterbacks can conclude all of those things that I have just said, knowing there will be flak damage to repair domestically in a free-information society. But, "objectivity can come back into fashion when the shooting is over."

Though the conclusions I've presented are derived from the strategies and tactics of both South Atlantic belligerents, there were some marked differences in their approaches.

- The disinformation from the British was intended to deceive the Argentines;

- The disinformation from the Argentine junta was intended to deceive the Argentine public;

- Both countries facilitated their disinformation through censorship but in different forms:

The British controlled their news largely by control of journalists' copy from the battle zone and by allowing speculation at home,

Whereas the Argentine junta controlled their news at the source of information, and that source was in Buenos Aires.

- The Argentines had a public information plan and a psychological action plan for this war;

- The British, like their operational efforts, were ad hoc in their approach to public affairs;

- The British particularly lacked technique and, therefore, training in their censorship program.

The war in the South Atlantic last year serves to remind us that information matters are an intrinsic part of war and should, therefore, form part of the planning for war.

War is something we train for with the hope of never having to do it. Public affairs in crises is something we often do but rarely, if ever, train for. Public affairs elements must be incorporated in military exercises in such a way that every level of command has to deal with the problem.

The field commander knows that he will be allowed less flexibility in decision-making the shorter the crisis is. That same decision-making process will have a vital impact on public affairs matters. We can read postmortems, but they will do us little good unless we train and prepare in every warfare specialty, including public affairs.

Lieutenant Commander Humphries, a public affairs specialist, is a student at the Naval War College and a member of the College's Falkland Islands study group.

JACK A. GOTTSCHALK

“Consistent with Security” . . . A History of American Military Press Censorship

Jack A. Gottschalk is with the New Jersey law firm of Morahan & Coppola. He is a former Assistant Essex County (N.J.) Prosecutor, a former Captain U.S.A.R. and Field Press Censor. He is an adjunct professor at Fairleigh Dickinson University.

In 1649 Parliament passed a law permitting the Secretary of War to license all army news. If no other purpose was served by the act, it was a precedent for censorship in the American colonies that officially began on May 13, 1725, when a Massachusetts Order-In-Council required that:

The printers of the newspapers in Boston be ordered upon their peril not to insert in their prints anything of the public affairs of this province relative to the war without the order of the government.¹

Given these actions, it is surprising that no censorship occurred during the Revolution, a point recalled by Thomas Jefferson in an 1813 letter where he wrote:

The first misfortune of the Revolutionary War induced a motion to suppress or garble the account of it. It was rejected with indignation.²

For whatever reason, although government-media relations in the nation's

1. JAMES RUSSELL WIGGINS, *FREEDOM OR SECRECY*, 94 (New York: Oxford University Press, 1964);
2. *Ibid.*, 94-95.

JACK A. GOTTSCHALK

early years were rocky (e.g., the *Philadelphia General Advertiser's* publication of the 1795 peace treaty with England was the "Pentagon Papers" incident of the time), pure military censorship apparently did not occur during the War of 1812, or during the Mexican War (1846–1848), the last American conflict where the idea of press censorship was not entertained, possibly because the war came too soon for the telegraph system.

By 1856, however, when Great Britain was fighting in the Crimea, telegraph communication had given war reporting unprecedented speed and, as Phillip Knightley relates in *The First Casualty*, military press censorship came with it.³ When the American Civil War began in 1861, both sides employed censorship widely, if not well.

Southern newspapers had more difficulties than did Northern ones. A lack of trained journalists, chronic paper shortages, and constant efforts to satisfy the Confederate government's stringent censorship created an enormous burden.⁴ But, while Southern censorship was rigid, it was, at least, consistent—a trait badly lacking in the North where censorship policy shifted on a daily basis.

Early in the war the Union government suggested a voluntary, self-imposed newspaper censorship, but the idea went largely unheeded primarily because no government censorship guidelines were provided. The effort at voluntary censorship having failed, the government subsequently moved to enforce a compulsory system that essentially consisted of after-the-fact (of publication) suspension of offending newspapers and close supervision of what was transmitted by the press over the far-flung system of telegraph lines.

Military actions against the press were numerous in the North and included the cases of the *New York Journal of Commerce* and the *New York World*. Both newspapers were suspended from publication for two days in 1864 because they published what turned out to be a forged letter—purportedly written by President Lincoln—that called for a 400,000-man draft in that year.⁵ On other occasions, several publishers were denied postal privileges by the government as a punishment for censorship violations, and General Ambrose Burnside shut down the *Chicago Times* for three days in 1864 because of its generally anti-administration editorial views. The suspension was lifted only after Lincoln countermanded Burnside's closing order.⁶

Censorship also generated among the media a distrust of government because of the use of censorship to stop the release of unfavorable news about

3. PHILLIP KNIGHTLEY, *THE FIRST CASUALTY* 16 (New York: Harcourt Brace Jovanovich, 1975).

4. JOHN HOHENBERG, *FREE PRESS/FREE PEOPLE*, 122–23 (New York: Columbia University Press, 1971).

5. *Ibid.*, 121.

6. *Ibid.*, 121–122.

American Military Press Censorship

command cowardice and bad judgment, a distrust not eased by the military's antipress attitudes. Early in 1862, for example, General Henry W. Halleck flatly refused to allow newspaper correspondents anywhere in his zone of command.⁷ Halleck was not unique. General William T. Sherman consistently kept reporters at a distance. Sherman based much of his opposition to the press on security considerations. In his opinion, the Confederate government obtained more intelligence from Northern newspapers than from its espionage efforts, a point that cannot be disregarded after noting the log entry written by Captain William Semmes, commander of the *C.S.S. Alabama*, a famous Confederate commerce raider. After capturing the *S.S. Manchester*, bound for Liverpool from New York, and aboard which Semmes found a number of Northern newspapers, he wrote:

"I learned from them [the newspapers] where all the enemy's gunboats were, and what they were doing. . . . Perhaps this was the only war in which the newspapers ever explained, beforehand, all the movements of armies and fleets to the enemy. . . ."⁸

Despite harassment and obstruction from Burnside, Halleck, Sherman, and others, correspondents continued to report, and newspapers continued to print the news—both good and bad. *The New York Times* summed up the issue during the war by noting:

More harm would be done to the Union by the expulsion of correspondents than those correspondents now do by occasional exposures of military blunders, imbecilities, peccadilloes, corruption, drunkenness, and knavery, or by their occasional failure to puff every functionary as much as he thinks he deserves.⁹

By April 1898, when William Randolph Hearst proudly took credit for war with Spain, better transportation enabled correspondents to reach places in days rather than weeks, and stories could be filed quickly because of ever faster communications. These journalistic capabilities created military censorship problems that were not properly addressed in the Spanish-American War, probably because of its brevity.

As in the Civil War, security was a problem. Correspondents aboard war-

7. *Ibid.*, 123.

8. JOURNALIST 3 & 2. RATE TRAINING MANUAL, NAVTRA 10294-C, Naval Training Command at 16-17 (Washington, D.C.: U.S. Government Printing Office, 1973).

9. HOHENBERG, FREE PRESS/FREE PEOPLE, 123-124.

JACK A. GOTTSCHALK

ships during the early days of the war freely cabled news about American ship movements and combat intentions, news that was released to Madrid as soon as it appeared in the daily newspapers. Clearly, some censorship was necessary and the result was the formation of naval censorship units that were established at Key West, Florida, Washington, D.C., and in seven cable offices in New York City.¹⁰ The nominal head of military censorship in New York by mid-summer of 1898 was Grant Squires, a former *New York Tribune* reporter who, as a civilian official, served in a liaison role between the military and news organizations. The Navy retained complete censorship control.

American naval censorship was imposed in 1914 at Vera Cruz following U.S. intervention there,¹¹ but no military censorship was used during the U.S. Army's expedition against the Mexican bandit-revolutionary, Pancho Villa, in 1916.

Once America entered the First World War in 1917, George Creel, a former newspaper editor (and a confidante of President Woodrow Wilson), was named to head the Committee on Public Information, the nation's newly formed propaganda and censorship agency headquartered on Jackson Place in Washington, D.C. Creel's management of domestic news censorship was based on a set of regulations prepared by the State, War, and Navy Departments before the United States entered the war.¹² These regulations, which the press voluntarily accepted, prohibited publication of such things as troop movements in the United States, ship sailings, and the identification of units being sent overseas.

Against the patriotic backdrop of the Creel Committee's activities appeared the Espionage Act of 1917 and the Sedition Act of 1918. The former was so broad that for the press not to have violated some portion of it would have been miraculous. Under its provisions, publishing any information that could be remotely considered as aiding the enemy or interfering with American military operations or war production was punishable by as much as twenty years in prison and a \$10,000 fine.¹³ And under the terms of the Sedition Act of 1918, any criticism of the conduct or actions of the American government or its military forces, including negative remarks about the flag, military uniforms, etc., could be similarly punished.¹⁴

Meanwhile, the chief American press censor serving in France with the American Expeditionary Force (AEF) was a former *New York Herald* reporter and Associated Press correspondent named Frederick Palmer, who had been personally recruited by General Pershing and directly

10. JOURNALIST 3 & 2, RATE TRAINING MANUAL, 15.

11. WIGGINS, FREEDOM OR SECRECY, 95.

12. *Ibid.*

13. HORNBERG, FREE PRESS/FREE PEOPLE, 182-183.

14. *Ibid.*

American Military Press Censorship

commissioned as a major assigned to public relations.¹⁵ Palmer was an excellent reporter, but his inability to handle the censorship problem quickly became clear. The correspondents accused him of not passing sufficient information, while the Army complained that he was not censoring enough.¹⁶

Palmer was soon replaced by a committee composed of ex-journalists, who had been commissioned as reserve officers for public relations duties, and Regular Army officers. The combination was chaotic and, in retrospect, it is amazing that only five journalists out of approximately sixty correspondents assigned to cover the war lost their AEF press credentials.¹⁷ The war nevertheless ended with a major censorship incident, the "False Armistice" story.

The military censors passed for publication a United Press dispatch filed by Roy Howard announcing the armistice a full four days before the real one was actually signed. Howard had filed his story based on information given to him by a reliable source, an American admiral at Brest, France. But, as a result of that story, the censors blacked out contact between the United Press in New York and Howard in France for three hours, thus stopping any possibility of correction, addition, or explanation.¹⁸ Interestingly, the end of the Second World War in Europe would involve another censorship blackout.

When war came to America in December 1941, some government censorship was already in operation. On December 31, 1940, Secretary of the Navy Knox formally requested the media to stop publishing any data about certain subjects (new ships, troop movements, etc.) without specific naval authorization; and in September 1941, both the Army and Navy announced that press censorship plans had been formulated to control information flowing from the United States in the event of a national emergency.

While the Roosevelt administration had formulated tentative censorship plans involving various executive departments and agencies including the Federal Bureau of Investigation and Federal Communications Commission, there was no central press censorship authority.

Pearl Harbor produced the jolt necessary for government action. On December 8, F.B.I. Director J. Edgar Hoover was given temporary powers to direct all news censorship and to control all other telecommunications traffic in and out of the United States. Simultaneously, President Roosevelt requested that the American news media voluntarily respect the Department of the Navy's censorship guidelines published a year earlier. Only eight days later, Roosevelt appointed Byron Price as Director of Censorship, relieving Hoover

15. KNIGHTLEY, *FIRST CASUALTY* 124.

16. HOHENBERG, *FREE PRESS/FREE PEOPLE*, 184.

17. *Ibid.*

18. KENT COOPER, *THE RIGHT TO KNOW*, 215-16 (New York: Farrar, Strauss & Cudahy, 1955).

JACK A. GOTTSCHALK

of that responsibility; and on December 18, 1941, pursuant to the War Powers Act, the President created the Office of Censorship with Price as its chief.

Since the Office of Censorship could only issue guidance relevant to domestic news censorship, it relied on the power of persuasion linked to a voluntary news censorship system that was worked out with the full cooperation of the media. The product of these labors was the *Code of Wartime Practices*, which became effective January 15, 1942.

The nation was hungry for war news and looked anxiously toward Washington, particularly during the grim, early days of the conflict. The Office of War Information (O.W.I.), created in June 1942 as America's propaganda agency, stood between the government and the press and was bound to feel severe stings of criticism from all quarters. Elmer Davis, the highly respected newsman and Director of the O.W.I., was powerless to force government agencies (including the military) to supply more accurate and timely non-sensitive information to the public, a situation that made relations between the O.W.I. and the media extremely tense. And it was military news censorship that caused many of the problems.¹⁹

The only theater in which American forces were actually engaged early in the war was the Pacific. There, a combination of MacArthur's almost dictatorial censorship²⁰ and the overtly antipress attitudes of Chief of Naval Operations Admiral Ernest J. King²¹ made attempts at news coverage difficult at best.

MacArthur's restrictive news media policy (e.g., multiple censorship of correspondent's copy before release)²² and his use of censorship for "image building"²³ were matched by the Navy's policy of delaying the news and then compounding the belated release by linking bad news with stories of combat success. While MacArthur got away with it, the Navy began suffering a loss of credibility.²⁴ The incidents of news management were not insignificant ones—e.g., news of the American naval defeat off Savo Island was released almost nine weeks after the battle.²⁵

The press, quick to recognize the government's heavy-handedness and suspicious that a lack of candor could mean a cover-up of military incompetence, bitterly complained of the Navy's attitude, particularly since the voluntary censorship program aided the Navy's attempts to manage the news. It fell to Davis to strike the delicate balance between picturing America's war

19. Lloyd J. Graybar, *Admiral King's Toughest Battle*, NAVAL WAR COL. REV., 40-43 (February 1979).

20. KNIGHTLEY, *FIRST CASUALTY*, 281-282.

21. Graybar, *Admiral King's Toughest Battle*, 39.

22. KNIGHTLEY, *FIRST CASUALTY*, 281.

23. *Ibid.*, 281-282.

24. Graybar, *Admiral King's Toughest Battle*, 40.

25. *Ibid.*, 40-41.

American Military Press Censorship

efforts in the best possible light while retaining the government's credibility with both press and public. Only after Davis successfully appealed to King (through Hanson Baldwin of *The New York Times*) did the Navy release news rapidly while remaining within reasonable security limits.²⁶ Davis's burden was, of course, not eased when early in 1942 Stanley Johnston, a *Chicago Tribune* correspondent who had learned of the Navy's ability to break the secret Japanese naval codes, inadvertently reported the names of Japanese ships involved in the Midway battle. When these names appeared in the newspaper the immediate fear was that the Japanese would know that their codes had been compromised. The fears were unfounded but, in the tenor of the times, the government referred the matter to a federal grand jury which refused to indict anyone concerned.²⁷

U.S. naval censorship in the Pacific continued to remain rigidly effective throughout the war. It was (and still is, as shown by the Falkland Islands campaign) far easier to censor news correspondents aboard warships. They are limited in their movement, contacts, and communications, and can only report what they are told by a command that frequently does not have the full story itself.

Despite MacArthur, the Army recognized that press censorship in Europe would require a different approach, and a special observer group had been sent to England in late 1941 to study recent British experience and to reach agreement with the British on a censorship policy that would become effective once U.S. forces entered the European theater. By the time the first American troops arrived in the United Kingdom in January 1942, the British and American representatives had completed their work, and joint censorship was a reality.

Four American officers initially constituted the entire U.S. military press censorship group, which was housed with British censorship at the Ministry of Information. By October 1942, when some officers were transferred to provide censorship support for Operation TORCH (the code name for the invasion of North Africa), there were ten officers and one enlisted man assigned to the London censorship office of the American military forces.

Taken in chronological order, American censorship of large-scale ground actions began with TORCH. To accomplish its censorship mission, the joint American-British military command assigned four censorship teams composed of both U.S. and British officers to the operation. One team was assigned to each of the three invading task forces, and one additional team was stationed at the Gibraltar headquarters.²⁸

26. *Ibid.*, 42.

27. *Ibid.*, 40.

28. PRESS CENSORSHIP IN THE EUROPEAN THEATRE OF OPERATIONS, 1942-1945 at 15 (Lodi, N.J.: 201st Field Press Censorship Detachment, USAR, reprint of SHAEF report, 1975).

JACK A. GOTTSCHALK

Censors went ashore with the landing troops, a necessity because accredited combat correspondents were also with the first assault waves and their news submissions had to be moved for censorship processing as quickly as possible.

The basic U.S. censorship guide during TORCH and the subsequent North African campaign was the previously noted *Code of Wartime Practices* as revised in June 1942 with supplements provided by the Office of Censorship and by the commanding officers of the various military theaters of operation.²⁹ Based on the procedures established in the *Code*, all new material was supplied in duplicate, first to public relations and then to the censors, a task that aggravated the media more than the censorship itself, particularly since the only alleged function of the military's public relations personnel was to transmit the copy once censorship had passed it for publication.³⁰

In addition to delay, other problems resulted from the sheer volume of news material and the lack of a sufficient military transmission capability to move the censored news to London and then to the rest of the world. But even when the organizational and transmission difficulties were finally remedied, news was unreasonably held up, often for a week in the censorship process, at Gibraltar, later in Algiers, and then again in London.³¹ Meanwhile, the correspondents noted that official press releases and communiqués were processed through censorship immediately and reached the homefront reading audience before the news reports.

But the single biggest problem to affect media-military relations in North Africa was the American use of field press censorship to block the release of political news. This "policy" censorship³² arose because of the turmoil caused by French colonial policy combined with violent antagonisms involving the Free French and the Vichy leadership.

The American State Department was opposed to the French government-in-exile headed by Charles DeGaulle. The U.S. supported General Henri Giraud, who, it was felt, would be easier to handle than DeGaulle in working with the Allies to stabilize North Africa. When it appeared that Giraud was not reliable, the United States began secret negotiations with pro-German Admiral Darlan, who controlled the French armed forces in North Africa. On December 24, 1942, Darlan was assassinated.

Meanwhile both the American and British news media had become increasingly vocal about North African events. Consequently, top U.S. military and diplomatic officials felt the urge to impose censorship on all political news from North Africa until the situation stabilized. The military

29. *Ibid.*

30. *Ibid.*, 16.

31. *Ibid.*, 16-17.

32. COOPER, RIGHT TO KNOW, 201-202.

American Military Press Censorship

view was that the uncertain political situation would encourage pro-German underground movements, and the diplomats argued that a news blackout would permit a political arrangement to be negotiated without concurrent public speculation. Thus the stage was set for Eisenhower to impose a strictly political censorship (which he later excused) that endured for six weeks, during which time the necessary agreements were reached between Giraud and DeGaulle.³³

In Europe, because of the lessons learned from North Africa, censorship training was emphasized and officers specially trained for censorship were assigned.³⁴ Gradually, along with the training of personnel, an updated censorship doctrine was developed, its basic thrust being that security was the prime news censorship consideration.

Organizational problems were also addressed as D-Day grew closer. A Joint Press Censorship Group composed of officers from the British, Canadian, and American forces was formed,³⁵ and an indoctrination course was held at the Chancellor's Hall in the Ministry of Information from April 10 to 21, 1944. Media and military notables, such as Edward R. Murrow, Brigadier General David Sarnoff and General Walter Bedell Smith, were in attendance.³⁶

At these meetings four primary objectives were chosen as the foundation of Allied press censorship operations: (1) security, (2) speed, (3) consistency, (4) censorship guidance and assistance to war correspondents.³⁷ On April 25, 1944, Operational Memorandum Number 27 was issued by Supreme Headquarters, Allied Expeditionary Force, which set forth the governing principle for the employment of field press censorship: ". . . That the minimum amount of information will be withheld from the public consistent with security."³⁸

There were over five hundred accredited combat correspondents in England by D-Day. Many went into France with the first landings. Others were dropped with the paratroopers behind German lines on the night of June 5, and still others were in bombers above the invasion or aboard the naval armada that bombarded the coast.

Submissions from bridgeheads established ashore reached censorship units located just behind the lines by courier, radio, and carrier pigeon. And censorship units at various levels had qualified linguists available to handle news copy that arrived in a dozen languages.³⁹ Three censorship teams, each including two Army, one Navy, and an Air Force officer, accompanied the

33. DWIGHT D. EISENHOWER, *CRUSADE IN EUROPE*, 153-54 (New York: Doubleday & Co., Inc., 1948; Garden City Books Edition, 1952).

34. *PRESS CENSORSHIP*, 37.

35. *Ibid.*, 43.

36. *Ibid.*, 46-50.

37. *Ibid.*, 55.

38. *Ibid.*

39. *Ibid.*, 60.

American Military Press Censorship

view was that the uncertain political situation would encourage pro-German underground movements, and the diplomats argued that a news blackout would permit a political arrangement to be negotiated without concurrent public speculation. Thus the stage was set for Eisenhower to impose a strictly political censorship (which he later excused) that endured for six weeks, during which time the necessary agreements were reached between Giraud and DeGaulle.³³

In Europe, because of the lessons learned from North Africa, censorship training was emphasized and officers specially trained for censorship were assigned.³⁴ Gradually, along with the training of personnel, an updated censorship doctrine was developed, its basic thrust being that security was the prime news censorship consideration.

Organizational problems were also addressed as D-Day grew closer. A Joint Press Censorship Group composed of officers from the British, Canadian, and American forces was formed,³⁵ and an indoctrination course was held at the Chancellor's Hall in the Ministry of Information from April 10 to 21, 1944. Media and military notables, such as Edward R. Murrow, Brigadier General David Sarnoff and General Walter Bedell Smith, were in attendance.³⁶

At these meetings four primary objectives were chosen as the foundation of Allied press censorship operations: (1) security, (2) speed, (3) consistency, (4) censorship guidance and assistance to war correspondents.³⁷ On April 25, 1944, Operational Memorandum Number 27 was issued by Supreme Headquarters, Allied Expeditionary Force, which set forth the governing principle for the employment of field press censorship: "... That the minimum amount of information will be withheld from the public consistent with security."³⁸

There were over five hundred accredited combat correspondents in England by D-Day. Many went into France with the first landings. Others were dropped with the paratroopers behind German lines on the night of June 5, and still others were in bombers above the invasion or aboard the naval armada that bombarded the coast.

Submissions from bridgeheads established ashore reached censorship units located just behind the lines by courier, radio, and carrier pigeon. And censorship units at various levels had qualified linguists available to handle news copy that arrived in a dozen languages.³⁹ Three censorship teams, each including two Army, one Navy, and an Air Force officer, accompanied the

33 DWIGHT D. EISENHOWER, *CRUSADE IN EUROPE*, 153-54 (New York: Doubleday & Co., Inc., 1948, Garden City Books Edition, 1952).

34 *Id.*, PRESS CENSORSHIP, 37.

35 *Id.*, 43.

36 *Id.*, 46-50.

37 *Id.*, 55.

38 *Id.*

39 *Id.*, 60.

JACK A. GOTTSCHALK

forces ashore on D-Day. Two teams were assigned to the U.S. forces and one to the British. A fourth team joined British forces several days after the initial assault on the beaches. Naval censorship was accomplished on the two command vessels of the invasion fleet.⁴⁰

The amount of copy submitted in the first days of the invasion was staggering. Upwards of 700,000 words were filed in color or feature copy alone. And overseas material arriving from France once the forces were ashore did not really begin to hit the Ministry of Information offices until almost forty-eight hours after the invasion began.⁴¹

On July 25, 1944, prior to the liberation of the French capital city, a major test of censorship practices occurred. During the opening phases of the attack on a German strongpoint at St. Lo, American ground troops were bombed in error by U.S. planes. One of the many fatalities was Lieutenant General Lesley J. McNair, and one of the first stories processed by censorship was written by Ernie Pyle, who had personally witnessed the incident.⁴² There was no attempt to cover the error, and thus censorship remained true to the policy stated before the invasion—that security was the only basis for censorship.

In August, Allied armies entered Paris and a new censorship headquarters was quickly established on the second floor of the Hotel Scribe,⁴³ although London remained the primary censorship clearinghouse for several weeks until Paris was completely secured. When that task was finally accomplished, London was officially designated as the "rear" censorship headquarters and Paris as the "main," an arrangement that continued for the rest of the European war.⁴⁴

The closing days of European action saw the greatest failure of military press censorship operations when measured against the much heralded censorship principles. The incident took place on April 11, 1945, at Ninth U.S. Army headquarters. American troops assigned to Combat Command B of the Second Armored Division had reached the western bank of the Elbe River. They were ready to move toward Berlin when they were abruptly halted by Ninth Army's commander, Lieutenant General William Simpson.

Shortly after returning to his headquarters, Simpson held a news conference but took the unusual step of ordering his press censor to stop any reports of what he was about to tell the media.⁴⁵ The general then told the correspondents that, acting under orders from Eisenhower as relayed by Omar Bradley, his units were not moving on to Berlin. Policy censorship

40 *ibid.* 61

41 *ibid.* 65

42 HORNBERG, *FREE PRESS, FREE PEOPLE*, 264

43 *PRESS CENSORSHIP* 81

44 *ibid.* 84

45 *COOPER, RIGHT TO KNOW* 203-206

American Military Press Censorship

under the guise of military security was thus employed as it would be a month later with the German surrender.

In his post-war writings, Eisenhower noted that:

Under the terms of the surrender document the heads of the German armed services were required to appear in Berlin on May 9 to sign a ratification in the Russian headquarters. The second ceremony was, as we understood it, to symbolize the unity of the Western Allies and the Soviets, to give notice to the Germans and to the world that the surrender was made to all, not merely to the Western Allies. For this reason we were directed to withhold news of the first signing until the second could be accomplished.⁴⁶

One American reporter, Edward Kennedy of the Associated Press, felt that there was a definite need to release the surrender news to a war-weary world. Kennedy avoided censorship by calling his story to London from SHAEF headquarters in Paris. London censorship passed the surrender news and the Associated Press in New York put it on the wire.⁴⁷

After the Kennedy story was published, SHAEF suspended all Associated Press coverage in Europe for eight hours—and Kennedy was fired.⁴⁸

The introduction of American military power onto the Korean peninsula in June 1950 caught the nation and its media off balance. Television was still in its infancy, but print, radio, and newsreel correspondents (eventually numbering over three hundred) arrived with the troops, often embarking from the same port—Tokyo. At first, press censorship was completely voluntary, a sort of gentlemen's agreement between the military and the press. This arrangement lasted from June 1950 until late December of that year when field press censorship was placed in effect.

It has been argued that the voluntary system failed because the competitive nature of the news business forced correspondents to commit serious security violations. Some of the military complaints during the voluntary censorship period were that news representatives, after being trusted by briefing officers, had prematurely announced the arrival of certain major American units in Korea, tactical troop movements, the initial recovery of American prisoners from the Chinese, and the use of the F-86 Sabrejet fighter for the first time in combat.⁴⁹ But the initial media restrictions were not solely based on security, and the guidelines were vague. When stories about panic,

46. EISENHOWER, *CRUSADE IN EUROPE*, 472

47. COOPER, *CRUSADE IN EUROPE*, 211-212, 219

48. *ibid.*, 216, 221, 222-224, 231-233

49. MELVIN B. VOORHEES, *KOREAN TALES*, 104 (New York: Simon and Schuster, 1952)

JACK A. GOTTSCHALK

inferior U.S. equipment, and South Korean civil corruption were published, censorship became inevitable.

Once censorship headquarters was established at Eighth Army, the previous practice (under the voluntary system) of having correspondents file their copy and photos with Tokyo either by military communications channels or via cable directly to the United States was stopped. All news material, including film, had to be passed by the Eighth Army's censors. The Air Force followed the Army's lead, operating through a security division in its Korean public information office. Both the Army and Air Force censorship organizations were headed by lieutenant colonels.⁵⁰

It did not take long for jurisdictional problems to develop. On January 11, 1951, Far East Command in Tokyo, which had been part of the censorship program along with Eighth Army, bowed out of the picture, leaving censorship completely to field army control. Apparently, during the ensuing sixty days, the field army did not censor enough, because on March 13, Tokyo headquarters announced that it was going to review all news material passed in the field for publication. This "multiple censorship" concept, which had been carefully avoided (except for MacArthur's South Pacific Theater) during the Second World War, remained in effect until Far East Command finally relieved the Eighth Army completely of its censorship duties in the spring of 1951.⁵¹

The final organizational structure of Korean military press censorship was based on a letter of instructions issued by Far East Command on January 6, 1953. In that document, a Joint Field Press Censorship Group (JFPCG), Far East Command (composed of military press censorship detachments of the Army, Navy, and Air Force) was created. The head of the group (the Chief Field Press Censor) was responsible to the Public Information Officer of the Far East Command and was assisted by deputy chief censors representing the Army, Navy, and Air Force. The chief censor's duties included supervision and implementation of field press censorship with regard to all United Nations and Far East Commands.⁵² In order to carry out its function, the Joint Field Press Censorship Group stationed detachments at Far East Command, Eighth Army and Fifth Air Force Headquarters and at the Panmunjom armistice negotiation site.

Some examples of political censorship used in Korea were noted by Robert C. Miller, who wrote in the *Nieman Reports* that the news media were not permitted to:

50 FIELD PRESS CENSORSHIP, FM 45-25, OPNAVINST 5530.5, AFM 190-5, at 58 (Washington, D.C., Departments of the Army, Navy, and Air Force, 1954).

51 VOORHEES, *KOREAN TALES*, 112-113.

52 FIELD PRESS CENSORSHIP, 45-50.

American Military Press Censorship

... mention the actions of South Korean police who blackmailed innocent farmers, threatening to arrest them as Reds unless they paid off. Hundreds fled into the mountains and joined guerrilla units because of police blackmailing tactics, but stories concerning this were killed....⁵³

The Korean censorship was so political in tone and so rigidly enforced that deliberate covert efforts were made by some reporters to avoid it. In the book *Korean Tales*, Melvin B. Voorhees, who as a lieutenant colonel headed the Eighth Army's censorship operation, recalled how correspondents employed a technique called the "Twenty Questions Trick" (a telephone code used between Korea and Tokyo, where the news media bureau offices were located) to get past censorship.⁵⁴

In July 1953 the armistice ending the Korean War was signed. The Army created a field press censorship capability in the reserve even before the conflict was over. At the Department of Defense level, the responsibility for supervising military press censorship was given to the Assistant Secretary of Defense for Public Affairs, and in August 1954 the Department of Defense published a joint service manual entitled *Field Press Censorship* with the following designations:

Department of the Army Field Manual FM 45-25
 Department of the Navy OPNAV INSTRUCTION 5530-5
 Department of the Air Force Manual AFM 190-5

This joint service manual was to be the standard procedural document for censorship organization and operations should the military again be required to implement a media security program.

During this period each of the service departments moved ahead independently with information security planning. In the Air Force, an Office of Information, reporting directly to the Secretary of the Air Force, was designated as the top-level public relations authority, with censorship being accorded a minor role. The Navy's information program was set up within the Department of the Navy's Office of Information and headed by the Chief of Information, who was also the public affairs adviser to the Chief of Naval Operations. Neither the Air Force nor the Navy maintained a manned press censorship organization within their respective active or reserve components.

53. PAUL BLANSHARD, *THE RIGHT TO READ*, 120-21 (Boston: The Beacon Press, 1955).

54. VOORHEES, *KOREAN TALES*, 106-107.

JACK A. GOTTSCHALK

Public information planning and organization had been refined (with the Army having the only media censorship capability) by the time of the Cuban Missile Crisis in October 1962. Within an hour of President Kennedy's October 22 address to the nation in which he announced the presence of Soviet missiles in Cuba, the Army's field press censorship detachments were partially and quietly mobilized.⁵⁵

In terms of manpower, these units included less than three hundred officers and men. Of that number, only five officers were requested to report for immediate active duty at Headquarters, Continental Army Command (CONARC), located at Fortress Monroe, Virginia. While all members of the units unquestionably would have been called to duty had hostile action occurred, only these five officers were initially contacted. Three of them remained on duty for the three days of the crisis and two stayed with CONARC for five weeks.⁵⁶

The decision to alert these units was based on the determination of the Joint Chiefs of Staff that the Army be ordered to prepare for possible field press censorship in the southeastern United States. A headquarters had to be organized for this purpose together with field press censorship teams of sufficient size to meet the needs of an estimated two hundred fifty correspondents. In the final analysis, contingency plans were developed that envisioned only the southern half of Florida as an active combat area.⁵⁷

Planning for this potential censorship task included the designation of Orlando, Florida, as the location for processing and censoring of still news photos, with motion picture and television film to be flown to the Department of Defense in Washington, DC., for censorship action. All news copy submissions were to be handled by field press censorship teams located within the combat area. The reserve officers were ordered to prepare censorship plans for use by the Army of the Atlantic (ARLANT) and the air and naval forces in the area (CINCLANT).⁵⁸ Had these plans been used, military press censorship would have become a reality on American soil for the first time since the Civil War. The crisis ended, of course, and the censorship planning involved with it became a largely unknown part of history.

Almost as soon as the United States entered the Vietnam War on a massive scale in August 1964, media censorship for purposes of military security became a Pentagon planning consideration. Early in the war, the Army placed a colonel from its reserve field press censorship detachments on active duty and sent him to South Vietnam for the purpose of assessing the situation and reporting on the feasibility of implementing field press

55 Carl M. Justice, former Commanding Officer, 211th Field Press Censorship Detachment, USAR, Conversation with author, November 10, 1981

56 *Id.*

57 *Id.*

58 *Id.*

American Military Press Censorship

censorship. Concurrently, discussions on the subject were held between the Department of Defense and General William Westmoreland, commander of U.S. forces in Vietnam.

Barry Zorthian, who later became a senior member of Time, Inc., served in Vietnam as director of the Joint United States Public Affairs Office (JUSPAO) and as minister-counsellor for information in the American embassy in Saigon. He has revealed that censorship was often considered in Vietnam and that the idea was rejected each time for practical reasons.⁵⁹ Zorthian is on record as having been personally opposed to media censorship there, although he acknowledges that his views may have represented the minority position.⁶⁰

Zorthian's views seem justified by the fact that the press voluntarily observed the military security rules that were established even though the conflict was unpopular with the media and the public. In over four and one-half years and in dealing with approximately two thousand news media representatives, only six security violations were considered by the military to be serious enough to involve the loss of Department of Defense accreditation, Zorthian has noted.⁶¹

Obviously, given the government's desire for censorship as compared to its repeated decisions not to employ it, there had to be some very cogent reasons for the lack of implementation. It is submitted that these reasons were political and logistical.

During the Vietnam War, television film was shot, processed, and shown to American audiences within twenty-four hours. Even if all combat film had been censored by the military, the war—which was being fought without a clear purpose or goal—would eventually have become a target of severe public criticism. Censorship would simply have delayed an inevitable reaction.

In addition, the military did not control the movements of civilians in South Vietnam. Each day, airliners landed and took off from Saigon airport, and anyone with the desire (and money) could hire a private plane to fly over the country. Unless all movement and means of transportation had been stringently controlled by the military (as in the Second World War), nothing could have prevented news correspondents from going anywhere in South Vietnam on their own. Similarly, any media representative with a news story stopped by censors (had censorship been in effect) could have boarded a civilian plane for the United States (or any other place) and filed the story regardless of censorship. As long as the reporter was no longer individually subject to military jurisdiction, the only possible punishment was the loss of Department of Defense press accreditation.

59 Barry Zorthian, *The Dimension of Communication: PERSPECTIVES IN DEFENSE MANAGEMENT*, Industrial College of the Armed Forces, 5-6 (February 1969).

60 *ibid.*, 5.

61 *ibid.*, 4.

JACK A. GOTTSCHALK

In June 1971 the Department of Defense moved to disassociate itself with the word "censorship" when it issued Directive 5230.7 wherein the Pentagon replaced "censorship" with the less provocative term "Wartime Information Security Program" or "WISP." The directive defined both the National Wartime Information Security Program and the Field Press Wartime Information Security Program as follows:

National WISP. The control and examination of communications entering, leaving, transiting, or touching the borders of the United States, and the voluntary withholding from publication by the domestic public media industries of military and other information which should not be released in the interest of the safety and defense of the United States and its Allies.

Field Press WISP. The security review of news material subject to the jurisdiction of the Armed Forces of the United States, including all information or material intended for dissemination to the public.⁶²

The document provided for the implementation of National WISP, *i.e.*, censorship, through the National Censorship Agreement entered into on October 1, 1963, between the Department of Defense and the Office of Emergency Planning (now the Federal Emergency Management Agency). Under its provisions, in any national emergency where domestic censorship was invoked, an Office of National WISP (similar to the Office of Censorship during the Second World War) would be activated. Initial personnel for this censorship organization would be provided by the Department of Defense and subsequently augmented by members of the National Defense Executive Reserve (NDER), civilian public information executives pre-assigned to perform the public media censorship task.⁶³

In a letter dated May 15, 1978, from the Office of the General Counsel, Department of Defense, to William M. Nichols, General Counsel, Office of Management and Budget, the reasons were set forth for a modification of Executive Order 11490. Executive Order 11490, which had gone into effect on October 28, 1969, assigned the Department of Defense responsibilities under the terms of the National Censorship Agreement.⁶⁴ According to the letter, the House Committee on Government Operations heard testimony

62 Arthur J. Simpson, Jr., *Wartime Public Media Censorship* at 10 (Unpublished essay, Carlisle Barracks, Pa.: U.S. Army War College, 1971).

63 *Ibid.*, 11-14.

64 Letter from general counsel of the Department of Defense to William M. Nichols, general counsel, Office of Management and Budget, May 15, 1978.

American Military Press Censorship

during 1972 from representatives of the Office of Emergency Planning that cast official doubt on the need for WISP short of a nuclear attack. Because of that testimony and the nonemployment of WISP during both the Korean and Vietnam conflicts, the House Committee on Appropriations directed in its 1974 Report on the Department of Defense Appropriations Bill that the reserve WISP units of the Army, Navy, and Air Force be phased out by June 30, 1974.⁶⁵

On January 30, 1975, the letter states, the Department of Defense asked the Federal Preparedness Agency (now also part of the Federal Emergency Management Agency) to rescind the National Censorship Agreement.⁶⁶ The Federal Preparedness Agency and the Department of Defense then became involved in discussions seeking to create another national WISP structure that could operate without the use of Department of Defense personnel, all national WISP units having been deactivated in fiscal year 1974 after appropriations for their existence were denied by Congress.⁶⁷

Apparently, the discussions between the concerned government agencies were not productive because on June 3, 1981, William H. Taft, IV, general counsel, Department of Defense, wrote to David Stockman, director of the Office of Management and Budget, stating that the Department of Defense wanted to amend Executive Order 11490 in order to be relieved of responsibilities more appropriately assigned to civilian agencies.⁶⁸ Subsequently, on November 27, 1981, General Richard G. Stilwell, (Retired), Office of The Under Secretary of Defense, sent a memo to each service secretary and to the Chairman of the Joint Chiefs of Staff stating that:

It should be noted that in 1974, the House and Senate Committees on Appropriations concurred that "it is unlikely *that any element of WISP* would be implemented in any contingency," and deleted all funds for participation by reserve personnel in WISP training. The WISP reserve units were subsequently disbanded in that same year.⁶⁹

The Stilwell letter is most interesting, particularly depending on how one interprets the phrase "*any element of WISP*," since the Army Reserve field press censorship detachments were operating until April 1977 and certainly funds were being expended for that purpose. In any event, it appears that the

65. *Ibid.*

66. *Ibid.*

67. *Ibid.*

68. Letter from William H. Taft IV, general counsel of the Department of Defense to David A. Stockman, Director, Office of Management and Budget, June 3, 1981.

69. Memo from General Richard G. Stilwell, USA (Retired), November 27, 1981.

JACK A. GOTTSCHALK

use of military WISP in Korea and certainly in the Cuban Missile Crisis was ignored. There is no question that the 1972 hearings and the fiscal year 1974 appropriations decision, together with the Pentagon's questions (after Vietnam) as to whether field press censorship could again be effectively employed, led to the decision to eliminate America's only military censorship capability represented by the Army Reserve units in 1977. However, despite the Army's view that technology has made field press censorship obsolete, it has been used by Israel during its recent Lebanon campaign⁷⁰ and by the British during the Falkland Islands fighting.

These recent and clearly perceived needs for media censorship by military authorities in democratic nations may well indicate that our own history of military press censorship is not yet complete. America's global commitments and the possibility that despite (or because of) nuclear weapons a Third World War might be largely or totally conventional require that we still heed the Supreme Court's words in *Near v. Minnesota*:

No one would question but that a government might prevent actual obstruction to its recruiting service or the publication of the sailing dates of transports or the number and location of troops.⁷¹

In summary, the media and the public, respectively, must remain determined to inform and be informed. The media and public also must be aware that our national interests may at some future time again require the use of media censorship "consistent with security" by military and civil authorities.

70. TV Guide, July 5, 1982, A-1.

71. *Near v. Minnesota*, 283 U.S. 697, 716 (1931).

Thursday, October 27, 1983

The Washington Post AU

U.S. Troops Remove 4 Reporters

Washington Post Foreign Service

Three American and one British journalists attempting to cover the invasion of Grenada by U.S. forces were evacuated from that Caribbean island in U.S. helicopters Tuesday afternoon when a local U.S. military commander decided they were in danger, Pentagon officials said yesterday.

Edward Cody, Miami correspondent for The Washington Post; Don Bohning of The Miami Herald; Morris Thompson of Newsday, and British reporter Craig Chamberlain were flown to the USS Guam, a helicopter carrier supporting the U.S. and Caribbean forces on Grenada, where they remained last night, incommunicado and unable to contact their home offices.

Three other newsmen, Time Magazine correspondent Bernard Dickstein, a New Zealand citizen; Time photographer Claude Urvac, believed to be a French national, and Hugh O'Shaughnessy, correspondent of the Financial Times of London, were still missing and presumed to be in Grenada.

The seven journalists flew from Barbados to Union Island, about 30 miles north of Grenada, on Monday and chartered a fishing boat to take

them to Grenada, where they arrived on Tuesday morning, the day of the invasion.

A Pentagon spokesman, Col. Robert O'Brien, said last night in the first official word their offices had received, that the four taken aboard the Guam would be transported to Barbados "when feasible." He offered no explanation as to why their home offices had not been informed that they were in U.S. custody for more than 24 hours after they became, in effect, the first American citizens to be evacuated from Grenada.

O'Brien also said he had no answer to questions concerning why the correspondents had been taken off the island when they encountered U.S. forces, nor why they could not be put in contact with their offices or allowed to file dispatches from aboard the ship.

The Pentagon statement came on a day when American news organizations began to voice increasingly sharp statements about Pentagon management of news from Grenada, and refused to allow journalists to be on the island.

News about the four came after two days of inquiries from The Washington Post, The Miami Her-

ald and Newsday at the Pentagon, the State Department and the White House. During that period, spokesmen for those agencies imparted various items of information. One report received by The Washington Post from the State Department early yesterday morning—a number of hours after the four apparently were in U.S. government hands—said that, according to a ham radio operator in touch with both State and American medical students on the island, the entire group of journalists were safe and in a hotel in St. George's.

Subsequent reports obtained by The Miami Herald from other ham operators said the journalists were in the custody of the Grenadian military. Reports of heavy fighting in St. George's increased concern among the newspapers that the U.S. units engaged in taking the capital might not know of the journalists' presence, perhaps in enemy custody. A spokesman for the State Department's Grenada task force said at that time that the commander of the overall Grenada operation, as well as his military superior, had been given a list of the names of the missing journalists and presumably had passed it down the line of command.

"Invasion Secrecy Creating a Furore; Spokesman Complained in Memo" Post 10-27-83

By LARI CANNON and David Hoffman

In its efforts to keep the invasion of Grenada a surprise and then to present it in the most favorable light, the Reagan administration has engaged in a campaign of secrecy and news orchestration that has created conflict inside the White House and a bitter confrontation with the media.

White House spokesman Larry Speakes, described by one official as "furious" after being misled about U.S. plans to invade the Caribbean island, complained in a memo to White House chief of staff James A. Baker III, deputy chief of staff Michael K. Deaver and White House counselor Edwin Meese III, that "the credibility of the Reagan administration is at stake."

It was also reported that Speakes and other administration press officials were so upset about being misled that they discussed the possibility of resigning.

Speakes confirmed sending the memo but strongly denied that he had discussed resigning.

In addition to the Pentagon refusal to let journalists accompany the invasion force, it allowed only one journalist to travel to the island since the mission began. Four western journalists were held incommunicado.

Three of them are Americans who were on the island at the time and were picked up by the U.S. invasion force and transported to the USS Gann offshore. They were being held there last night.

The four include correspondents for The Washington Post, The Miami Herald and Newsday.

Three other journalists, including a correspondent and photographer for Time magazine and a reporter for the Financial Times of London, had arrived with the four by boat Tuesday morning. They became separated from the group while on Grenada, and their whereabouts on the island are unknown. [Details on Page A11]

Meanwhile, media representatives objected to the Pentagon policy of refusing to allow reporters into the war zone in Grenada. Responding to this outcry, the administration decided last night to allow reporters onto the island.

"It's our view that this should be covered by the press from now on," Baker said.

Officials said that access to Grenada was

See SECURITY, A14, Col. 1

supported in private meetings Tuesday by White House communications director David R. Gergen and then by Baker and Deaver, but that the Joint Chiefs of Staff resisted until it was clear that the invasion was a success.

The formal explanation given by both the White House and Gen. John W. Vessey Jr., chairman of the joint chiefs, was that reporters were barred for their safety. However, officials acknowledged that no such action had been taken in Vietnam, El Salvador or Lebanon, where the danger was greater.

The conflict between the administration and the news media developed on two levels yesterday.

One was the clamor from the media to enter Grenada to obtain news more than the official view of the invasion.

The other was a conflict between White House reporters and Speakes over his comment on the eve of the invasion. He responded to a CBS query about whether Marines had landed on Grenada by saying it was "preposterous."

Despite his private memo to Baker and other top advisers, Speakes publicly defended the conduct of the administration in throwing a blanket of secrecy around the invasion.

"The policy of the White House is to tell the truth," he said. He admitted, however, that his answer to the invasion question could have caused confusion.

Neither Speakes nor Gergen was informed about the invasion until 6 p.m. Tuesday, when the invasion was underway.

The guidance for his remark "preposterous," Speakes said, came from Bob Sims, press officer for the National Security Council, who had obtained it from John Poindexter, the deputy national security adviser.

High administration officials said that they did not know whether Poindexter had acted on his own or had been instructed to give the misleading guidance by national security adviser Robert C. McFarlane. Neither Poindexter nor McFarlane responded to requests for comment.

Using "preposterous" to refer to a landing on Grenada first came from Poindexter in guidance to Sims, who was responding to a query from CBS correspondent Rob Schieffer.

"No one put it to me in the bureau news," Sims said. "I was never asked

by reporters whether there would be an invasion."

Sims said that he was tired and overworked from responding to questions about Lebanon, and didn't make further inquiries, as he might have done under other circumstances.

Several officials said that the pre-occupation of the news media with Lebanon, where more than 200 Marines were killed in a suicide bombing Sunday, contributed to the White House effort to shroud the Grenada invasion in secrecy.

"Everyone was overworked and focused on Lebanon," said one official, "including the press, the White House staff and probably even the president."

But after the invasion occurred, the administration promptly launched a largely successful campaign to persuade the American public that the invasion of Grenada was a measured response to a request from neighboring nations.

Their primary weapon was Eugene Charles, the articulate prime minister of Dominica, who appeared with Reagan in the White House briefing room Tuesday morning when he gave his reasons for the invasion.

A White House official said with pride last night that Charles had been on all the evening network news shows Tuesday, on ABC's "Nightline," on two network talks shows the next morning and had been interviewed by USA Today and U.S. News & World Report.

In addition, the White House supplied a number of spokesmen, including Secretary of State George P. Shultz and Defense Secretary Casper W. Weinberger, to explain the administration's position on the invasion. "We had a whole phalanx of people out there," Gergen said. "The part of the process, and there's nothing unusual about it, though it was intense."

Although the orchestration of the administration's position was untypical of past efforts, this time it occurred against the backdrop of the news blackout in Grenada, which meant that virtually the only news coming out on the invasion was the official White House version.

Administration officials at the level debated the orchestration of the approved press. At Weinberger's at a news conference, that the invasion had been carried out in secret

Grenada News Orchestration Hit by Media, Press Aides

POST

SECURITY, From A14

10-27-83

But some officials said that the White House may pay a long-term price for, as one of them put it, "advertising that our press officials just aren't told what is going on."

The official reason for Speakes and Gergen being kept in the dark about sensitive information is that then neither is thus put in the position of lying. In practice, it has meant that these and other officials sometimes give out inaccurate information because they obtain their guidance unofficially and are not informed by Baker or Deaver.

Speakes made this point in his memo to Baker, describing what had happened and concluding: "This comes from having too little information." It was learned that Speakes, press office foreign policy spokesman Les Janka and Sims were so frustrated by the incident that they actively discussed resigning.

Gergen, who was not involved in the Grenada guidance but was an

active participant in the effort to change the policy excluding reporters from Grenada, was also reported to have considered quitting.

But there was no indication that White House officials, who have often dealt with their own communications officials on a need-to-know basis, and sometimes less than that, would change their policies.

At the early morning briefing yesterday Speakes held up several typewritten pages of questions from the previous day's briefing that he said he was trying to get answered. Later Janka said, "We don't have all the facts."

Weinberger defended the decision not to let reporters on Grenada as the decision of commanders in the field. "Their conclusion was they were not able to guarantee any kind of safety to anyone," he said. "We just didn't have the conditions under which we would be able to detach enough people to protect all of the newsmen, cameramen, gripmen and all that."

"Administration Limits News of Grenada"

By PHIL GARLEY
Special to The New York Times

WASHINGTON, Oct. 26 — For the last two days, the Reagan Administration has barred reporters from Grenada and imposed extraordinary restrictions on news coverage of the military invasion of that Caribbean island.

As the military operation by United States and Caribbean nations continued for a second day, President Reagan said through a spokesman that reporters would be allowed onto the island when American military commanders determined that conditions were safe for them. Defense Secretary Casper W. Weinberger said he hoped the island could be opened to reporters as early as Thursday.

Until late this afternoon, when Secretary Weinberger and Gen. John W. Vessey Jr., Chairman of the Joint Chiefs of Staff, provided the first detailed briefing of the operation at a news conference, reporters here and elsewhere had based themselves relying heavily on ham radio operators and Radio Havana for reports on conditions on the island.

It was ham radio operators who reported today that six journalists, including two Americans, had landed on the island in a chartered fishing boat. First reports said the journalists had been taken to the St. James Hotel in St. George's, the capital, but later reports said at least four of them had been taken from the island by American forces to the carrier U.S.S. Gann.

Meanwhile, the Federal Communications Commission moved to clamp down on ham operators, who have been providing much of the information to the press and the public about the situation in Grenada. William Russell, a spokesman for the commission, said some of the operators had been using unauthorized frequencies to pick up broadcasts from the island, and that the commission had started monitoring operators for such violations.

Defense Department officials, who spoke on the condition that they not be named, said that Britain's tight control over press coverage of its war with Argentina over the Falkland Islands last year had made an impression on some American military commanders, particularly General Vessey. He has told reporters in the past that he believes there is too much news coverage of the military.

"The President and Secretary Weinberger are backing their commanders on this thing," one Defense Department official said.

During the war over the Falklands, British reporters were allowed aboard British ships and were allowed onto the island with the invasion force. They reports, however, were censored by British censors.

There was no United States involvement in the Vietnam War. To get credits from U.S. military authorities, reporters had to sign a pledge not to disclose in advance troop movements, exact casualty totals and certain aspects of military operations.

At today's news conference, Mr. Weinberger said the operation's military commanders had decided they did not want reporters along, and he added that he "wouldn't ever dream of overriding a commander's decision."

He added, "Their conclusion was that they were not able to guarantee any kind of safety of anyone" because of uncertainty over what kind of conditions they might encounter.

"Need for Surprise"

Asked if there was concern about how the public might react to television coverage of the fighting, the Secretary said: "I think one of the most important reasons that we didn't is the need for surprise in this operation. We were going in there very quickly and we needed to have surprise in order to have it successful."

Some of the country's major news organizations, including most of the television news and wire services, had protested the news coverage restrictions in letters to President Reagan and other Administration officials.

In a letter to Mr. Weinberger, Edward M. Joyce, president of CBS News, wrote: "I would like to protest the attitude expressed by your Public Affairs office as indicated in the statement to our correspondent Bill Lynch that 'we learned a lesson from the British in the Falklands.'"

"I'm screaming about it because writing letters takes too long," said Howard Simon, managing editor of The Washington Post. "I think a secret war, like secret government, is antithetical to an open society. It's absolutely outrageous."

Mr. Simon said one of his newspaper's reporters, Edward Cody, was among the six journalists who reached Grenada by boat. He said he had been told that Mr. Cody had been taken off

Television news organizations this week made the events in Grenada and Lebanon the subjects of instant foreign policy analysis. Page C31.

the island to the carrier Gann. Also reported to be on board the carrier were Don Robinson of The Miami Herald, Merrill T. Simpson of Newsday and Bernard D. ... of Time magazine. The identities of whereabouts of the other two journalists in the group could not be established.

Survivors Protest

Severin Topping, managing editor of The New York Times, said, "We have strenuously protested to the White House and the Defense Department about the lack of access to the story in Grenada by our correspondents who are waiting on Barbados. We also are disturbed by the paucity of details about the operation released by the Pentagon at a time when the American people require all the facts to make judgments about the actions of our Government."

N.Y. TIMES

10 27 83

President Reagan said reporters will be allowed on Grenada to such an extent that there are calm enough to be "consistent with safety requirements" agreed to by the Defense Department," according to Larry Speakes, the chief White House spokesman. Mr. Speakes relayed that word this afternoon, after he had agreed to take a request directly to the President from the White House press corps that reporters be permitted into Grenada.

Mr. Speakes said that another concern had been that "the presence of media there could distract commanders." That view was echoed by a senior Defense Department official who said that the invasion was a command-type operation that does not lend itself to what he called "the tender loving care and feeding of the press."

Acrimonious Briefing

Mr. Speakes' afternoon briefing was no less acrimonious than the morning session, as reporters asked for details on the invasion and were referred to the Pentagon. In particular, the reporters were frustrated in their attempts to track details of the Administration's reported eleven-hour diplomatic response to possible attempts by the revolutionary council on Grenada to discuss safeguarding the Americans there.

Confusing and fragmentary information was offered, and Mr. Speakes, complaining about the accuracy of some news reports, strenuously refused to take additional questions from one reporter he considered annoying. "I'm tired of dealing with you," he said.

"You're carrying your management's water on this thing," he said to another reporter, who had asked why reporters could not go to the island.

News reporters were concerned at having been misled by the White House's first denial of initial invasion reports, a situation Mr. Speakes said was not intentional. He was asked whether the Administration policy was to be selective in telling the truth. "The policy of the White House is to tell the truth," Mr. Speakes replied.

Jerry W. Friedheim, a former Assistant Secretary of Defense for Public Affairs, said "there are damn few precedents" for continuing the news restrictions beyond today. Mr. Friedheim, who is now executive director of the American Society of Newspaper Editors, said news coverage of the invasion would make it easier to the Administration to win public and Congressional support for the operation.

A former senior Defense Department official in the Carter Administration, who spoke on the condition he not be named, said, "I can't recall an overt military operation of this sort not involving some sort of press coverage, at least a press pool. This is very unusual."

U.S. Forces Thwart Journalists' Reports

By Edward Cody
Washington Post Foreign Service

ST. GEORGES, Grenada, Oct. 27—A group of seven journalists, including reporters for four American news organizations who arrived here Tuesday morning as U.S. invasion forces landed, tried unsuccessfully until today to report what was happening on Grenada. But their efforts were thwarted, first by technical communications blackouts on the island and later by the invading force itself.

We had left Barbados Monday by chartered aircraft to Union Island, north of Grenada, touched by boat to Carriacou, another island that is a Grenadan possession, and arrived on a separately seated small boat in Grenada just after the landing.

Initially detained by Grenadan forces, by the time we reached telephone and telex facilities in the town, the lines were dead.

It was early yesterday when, while wandering through the relatively peaceful Grenadan capital, three of us—myself and correspondents for *The Miami Herald* and *Newsday*—made our first contact with U.S. troops. By 2 p.m., a good-hearted marine colonel who had listened to our pleas to allow us to use American communications facilities to reach our home offices, arranged to have us flown to the USS *Gann* offshore on one of a number of helicopters ferrying back and forth to his position.

But by 10 a.m. today, we three reporters, who had been joined by a British colleague in the meantime, were being helicoptered back to the same landing zone we had left 18 hours earlier—still without getting our stories back to our newspapers.

The intervening time was a series of frustrations, pleasant conversations with sailors and marines aboard this helicopter carrier and repeated pleas to be allowed to use shipboard communications or to be transported to Barbados to use commercial telephone service from there. It was also a period in which we were constantly watched, even as we slept in crewmen's bunks with a sailor detailed to stay awake sitting beside us.

Vice Admiral Joseph Metcalf III—Second Fleet commander running the Grenada operation—first dispatched Cmdr. Tony Hilton to announce that the task force's communications were so busy with military traffic that we reporters had no chance of using them. After a request, he said he would do his best to get a message to at least one newspaper with a list of those of us who had landed on Grenada—including us four and the two reporters and one photographer who remained on the island.

Disappointed, we then suggested that we be carried on one of the frequent military flights between Grenada and Barbados to use the telephone there. Hilton, the fleet public affairs officer, said he would do his best.

A short while later, we were led aboard a helicopter and flown down from Point Salines, the Grenadan peninsula where a Cuban-built airport was being used by the U.S. invasion force. But just before the helicopter was due to take off from the busy flight deck, we were ordered to get out and were led back inside the ship to the commodore's wardroom.

Metcalf then came to greet us, apologizing for the switch and explaining it was because he was reluctant to risk sending civilians into a high-risk area. It was not clear whether he meant Grenada as a whole, where we had just spent two days, or Point Salines specifically, where the U.S. military was landing and taking off regularly.

In any case, we said we needed to file our dispatches and wanted to use shipboard facilities—the reason we had first come aboard—or go to Barbados. Metcalf replied he had to have the request cleared with Washington. By the time darkness fell, when Hilton said civilians could no longer fly on helicopters, the clearance had not yet come and dinner was served.

Reinforced by fried ham and a promise that we would be flown to Point Salines for a flight to Barbados "at the first light," we bunked down for the night. Up at dawn, we were told we would depart at 8:30 a.m. At 7:30 a.m., we were told we would leave at 10 a.m.

At 9:30 a.m., Metcalf appeared again to say

we reporters could accompany marines on to Fort Frederick, where he said "an operation" was due to take place against remaining Grenadan defenders, then fly to Barbados. Or, we could fly immediately to Barbados.

Seeking to complete our stories, we opted to accompany the Marines in the hope of catching a later flight to Barbados. On arrival back in Grenada, however, we met the *Time* magazine correspondent we had left on the island along with a photographer and another British reporter, who told us the fort had been undefended since the previous afternoon. At this point, we insisted on continuing to Barbados, where we arrived shortly after 2 p.m. today.

[The Washington Post made repeated inquiries for information about the whereabouts of the journalists—who had last been heard from when they departed Barbados Monday—throughout Tuesday and Wednesday to the Pentagon, State Department and White House.

[At about 2 p.m. Wednesday, White House Deputy Chief of Staff Michael Deaver told Post publisher Donald E. Graham, in response to a request from Graham for any information U.S. forces might have about Cody's whereabouts and safety, that the four newsmen were safe, aboard the *Gann*.

[Half an hour later, White House Director of Communications David Gergen telephoned *The Post* to say that he had been called by other news organizations if a Post reporter was missing in Grenada.

[At 8:30 p.m. Wednesday—eight hours after the journalists had arrived on the *Gann*—Col. Robert O'Brien of the Pentagon said in response to inquiries from *The Post* that the newsmen had been evacuated on Tuesday afternoon by the local commander for their own safety because they had wandered into a fire fight. A sketchier version of this evacuation report also had been relayed to a Post reporter by Deaver earlier in the day and was repeated to another Post reporter by a senior Pentagon official at midday yesterday. During this time the correspondents were not permitted to have direct communications with their offices.]

Friday, November 20, 1983

U.S. News Control' on Grenada?

Limited to Military Footage Networks Cry Foul Play

By Tom Shultz

I had been the little war that wasn't there—no there on the American television screen, when one would have expected to find it. Finally, last night, after a nationally televised address by President Reagan, networks aired the first glimpse of combat footage from the U.S. invasion of Grenada.

However, the footage showed very little combat. And it was official U.S. government-approved film photographed by the military and cleared by the Pentagon before being released to the networks. Military foot- age through the president's remarks. If hostilities in Grenada are winding down, the war between the press and the White House is dramatically heating up.

Three correspondents, one from each network, and one network "you" crew had been allowed into Grenada for the first time since the invasion early yesterday, and a military plane was to fly them back to Barbados by 5 p.m. so they could file stories for the nightly network newscasts. But at 8 p.m., when the president began his emotional appeal to patriotism, the press plane was still sitting there on a Grenada runway. It hadn't budged.

Military officials told the networks the plane had been ordered to stay in Grenada. See NETWORKS, B3, Oct. 9

The Grenada Footage

NETWORKS, From B1

couldn't take off because of excessive air traffic. But at all three networks, there was pointed speculation that this was just another facet of the administration's campaign to control the news from Grenada. The plane was held on the ground, it was the- re before the president spoke.

And network spokesmen said they found it strangely "coincidental" that even the innocuous footage shot and cleared by the military was not made available until the president's speech, thus preventing the networks from showing it until the speech had ended. Most of the film consisted of American students smiling, blowing kisses and flashing the "V" sign as they were escorted off the island under military protection. It looked like a bunch of kids going to camp.

NBC News anchorman Tom Brokaw said from New York last night, immediately after he left the air, that he thought the administration's actions in suppressing news of Grenada were "conscious" and sus- pected.

"I think it's outrageous," Brokaw said of the White House policy. "I don't know how it can be called any- thing else but managing the news. Everything they've released has been screened by the Pentagon—even the most benign kind of footage. It's fairly clear they want to 'keep a tight lid on this as possible.'"

When NBC showed the Pentagon- approved footage on the air, Brokaw emphasized to viewers that coverage of the invasion had been "lightly controlled" by the White House, and NBC correspondent Marvin Kalb during his analysis of the president's remarks accused the administration of "news management."

ABC was the first to air the foot- age—right after the president con- cluded his speech with "God bless



Reagan after his released speech; by Ray Justly—The Washington Post

foreign nation, not their own. Then CBS showed it last. Before showing it, anchorman Dan Rather told viewers that the film had been "shot by the Army and captured by the Army," and CBS emphasized the words "Cleared by Defense Dept. officers over the images."

After showing the film, Rather said two more times that the govern- ment had shot and "cleared" the film. The minute CBS left the air, its New York switchboard lit up with calls, some of them charging the network with being "unpatriotic" and others insisting the U.S. govern- ment would never censor anything, a CBS source said.

Howard Stringer, executive pre- sident of the "CBS Evening News," was asked if he thought the timing of the film's release and the delay of the plans from Grenada were part of a White House plot to suppress cov- erage of the story. He said, in effect, yes. "It makes one anxious, suspi- cious and a touch skeptical about the administration's attitude toward press coverage of the invasion," Stringer said.

Robert E. Frys, executive produc- er of "ABC World News Tonight," said, "We are very concerned about the control—to use a polite word—to assert on the coverage of the in- vasion. The concept of freedom of the press in this situation has not been adhered to. We have been to- tally blacked out."

While the president was on the air, stepping up and climbing out the old airplane, network news execu- tives in New York watched impatient- ly for news of the press plane. It did not land in Barbados until 8:48 p.m., more than 15 minutes after the pre- sident had concluded his speech.

A producer at one network said the administration's slow-walking had forced newsmen into the kind of journalistic espionage they might use- fully, positively, doesn't have to be- lieve their right away.

On Wednesday, friction between the White House and the news media exploded at a briefing held by White House spokesman Larry Spivak, at which ABC News White House correspondent Sam Donald- son angrily protested the black-out. Spivak reportedly became furious and called Donaldson "venomous" in the shouting match that ensued.

Reagan's speech was his usual grandstanding tour de force, one po- sition missing—as when speaking of tragic U.S. losses in Lebanon—and the next moment the stern ad- monisher, warning the Soviets and other foes against aggression. He ended with an anecdote that had already been reported by seemingly every news source in America. "May I share something with you I think you'd like to know?" the President asked the viewer, proceeding to tell the story of Marine Commandant Gen. Paul X. Kelley's visit to a wounded marine who wrote on a piece of paper "Semper Paratus."

"Always Faithful," Reagan said of the commandant. "He cried when he saw these words, and who can blame him?" Reagan himself seemed to be choking up. And who could blame him? Mean- while, at that moment, network news personnel were still combing news- worth over the lack of film and the White House efforts to control it.

If this is an attempt to manage the news, it is so far a stunningly successful one. It puts Nixon and Carter to shame. Future administra- tions will look back on it as one of the art.

In Barbados, a Restless Press

150 Miles From the War, The Bad News Is No News

By Phil McCoola

BRIDGETOWN, Barbados, Oct. 28—It's got all the elements—the bearded palm trees, the sugar cane waving in the hot sea breeze, the native taxi drivers careening down narrow streets, the expensive but classy hotels, the slowly rotating ceiling fans above ranks of sweating diners in dark restaurants, the blini-clad tourists on the beach, the U.S. combat troops walking around the airport with that special swagger. You almost expect Joel McCrea, the jaunty reporter-hero from Alfred Hitchcock's "Foreign Correspondent," to come wandering through.

It's also got 325 crazed journalists.

But this is Barbados, not Grenada.

"Seven days down here and it's been a bitch," said Time magazine photographer Michael Luongo, standing outside the old shambling airport building that has become the press center. "These liaison has been nil. We've had no briefings to speak of."

"Everybody in the press is outraged," said Newsweek correspondent Elaine Shannon in the air-conditioned restaurant at the airport, where she had sought a cheeseburger and respite from the heat. "I've never seen so much pent-up fury."

Of course, both Luongo and Shannon might be happier had they not been left out of the limited press pool that U.S. military forces flew yesterday and today from this island paradise 150 miles across an azure sea for a few hours' look at Grenada.

But of the 325 journalists from all over the world that U.S. officials said are here today, so far only about 35 have been given the limited press tour.

They are "pool reporters," which means that when they get back after their tour they are duty-bound to give all details of their reporting to their comrades in the press corps. The result is a madhouse, a frustrating mob scene.

"People were screaming 'Talk! Talk!'" Shannon said of last night's pool report. "Nobody could file because the flight was so

See PRESS, C3, Col. 3

PRESS, From C1

late coming back. We were faced with a pool report that quoted paratroopers who would not give their names quoting Grenadians as jumping up and down shouting, 'We're free!'

But the frustration is real, and what is happening here among the press, the soldiers and the U.S. government is strange and slightly unnerving. For example, a camouflaged trooper sitting at the airport here today was asked if he was a Ranger. He replied, with a curl to his lip, "I don't know, man."

"I've just never seen such a mad dog and pony show before," said a senior editor of a major media outlet who asked not to be identified. "I just think the g-damn thing is such a flagrant manipulation of the press. They keep talking about how they're concerned for our safety, which I find truly touching."

Carole Agas of Newsday said U.S. Embassy officials at the airport yesterday tried to confiscate her notes and interviewed officials that appear only she was not supposed to interview.

"I don't think you should release that—anything you hear here you can't write," Agas quoted an embassy official as saying. Agas said she failed to obtain complete identification of the embassy officials, and got out of the situation by laughing and saying, "Hey, come on fellows, let's be reasonable." She said she then walked away and the officials did not press the point.

Luongo, the Time photographer, had an even more hair-raising experience—this one with Barbados police officers who, he said, seemed to think he should not be taking photographs near the airport, where

THE WASHINGTON POST

Monday, October 29, 1983

C3

A Frustrated Press Waits in Barbados

U.S. military aircraft are plainly visible going about their operations. Luongo said he was detained and strip-searched. "I was personally interviewed, questioned about anything and because he was the only available military officer at 2:30 p.m., searched at the same time in a small room where police took them, he said.

"They didn't touch us . . . they wanted our film. We gave them because rolls."

Facilities at the press center, several miles outside of town, are minimal. Only about a dozen telephones are installed, and when the pool reporters returned last night all phone connections out of the island were jammed for hours.

The big, limousine-floored press room smells of stale sweat and is littered with trash. Reporters nervously fidget about some talking on the phone to their editors, others pumping information out of one another. The U.S. military command post for airport operations here is nearby, but there seems to be only minimal and quite formal relations between the press and the military.

The nearby airfield contains many C130 and other transport aircraft for ferrying U.S. troops to the combat zone, as well as transport and fighter helicopters. The whine of aircraft engines and the thumping of rotor blades form a continual backdrop.

For example, to find out how many reporters are here, one had to submit a written request. About an

hour later, a very polite Capt. Dean Chamberlain returned with the answer—325—but since he was new on the scene, and could not be substantively questioned about anything, and because he was the only available military officer at 2:30 p.m., room where police took them, he said.

Eventually Chamberlain emerged with a mimeographed "Grenada update," which he handed out to about 100 reporters.

"Between Oct. 26 and Oct. 27," the news release said, "all major military objectives on the island [of Grenada] are secured . . . Our forces have been well received by a friendly populace [sic] . . . the fighting is continuing."

About the time the news release was being handed out, there was a sudden flurry among the reporters as someone rushed into the room and shouted, "There are evacuees out front!"

There was a great scrambling and grabbing of cameras and other equipment as reporters rushed outside to see what was going on. Many evacuees from Grenada were there—it was not clear exactly how they got there, but as the press interviewed them, it was clear that they had been evacuated by American forces.

Most appeared to be not too happy about it. As cameras clicked and rolled and as microphones were thrust into her face, an evacuee who identified herself only as Maria said, "We're not happy because we

did not feel it was necessary for the American troops to invade Grenada. "How do the Grenadians feel?" shouted a reporter.

"They were very scared," said Maria.

Another evacuee, Kathleen Robinson from Coast Britain, was standing nearby. "Would you go back?" she asked.

"Once the Americans clear out, yes, I'll do it very much," Robinson said.

Another evacuee, a German who identified himself only as E. Back and who demanded that no photos be taken of him, said, "The opinion of most Grenadians is they want to finish it but they have such a strong anti-sympathy to the Americans that it will probably continue."

"He's an engineer," joked a cynical reporter, "and put 'em' terrorist."

Other reporters nearby laughed. "There's something strange going on here," said Luongo of these evacuees. "They won't talk much. They're making some gross exaggerations."

Another photographer, Alan Casey of Sipa Press, said, "Are they Capetians, these weirdo?"

Later, speaking of the American military, Casey said, "All this crap we need to be on the island!"

By 6:45 tonight, the press pool flew in at 5, had still not returned from Grenada. The press center was jammed with roughly 200 reporters growing more and more restless.

"What an abortion this thing is," said Tampa television correspondent Job North. "So many high [journalists] hopes dashed. I'm on sick of looking at sunset crews and forest crews and everyone else. I could throw up. I just want it to be over."

That seemed to reflect the mood of many of the people here, and as the minutes and missed deadlines continued to tick by, it proceeded to be a long, frustrating night.

THE WASHINGTON POST

Information Out of Sync

Marines Overpowered, Underfunded Capital

By Maxwell Cady

ST. CHARLES, Conn., Oct. 18.—The United States Marine Corps today is overpowered and underfunded in its campaign to retake the capital of the island of Cuba, according to a report from the United States Marine Corps.

While a few hours, barely spent, were devoted to the capture of the capital, the United States Marine Corps today is overpowered and underfunded in its campaign to retake the capital of the island of Cuba, according to a report from the United States Marine Corps.

The gap resulted in part from a lack of information on the part of the United States Marine Corps, according to a report from the United States Marine Corps.

Information Gap Creates Confusion on Aspects of Island Conflict



Thursday night was anything but a quiet one in the United States today, as the United States Marine Corps reported that it had captured the capital of the island of Cuba, according to a report from the United States Marine Corps.

As we walked, circumstances were... The United States Marine Corps reported that it had captured the capital of the island of Cuba, according to a report from the United States Marine Corps.

ATTACK, FROM A1

...to have been in part from the... information's retention in... Cuba, according to a report from the United States Marine Corps.

...the United States Marine Corps... information's retention in... Cuba, according to a report from the United States Marine Corps.

...the United States Marine Corps... information's retention in... Cuba, according to a report from the United States Marine Corps.

...the United States Marine Corps... information's retention in... Cuba, according to a report from the United States Marine Corps.

...the United States Marine Corps... information's retention in... Cuba, according to a report from the United States Marine Corps.

ABROAD AT HOME

What Was He Hiding?

By Anthony Lewis

BOSTON, Oct. 30 — A man who strains to conceal what he is doing must fear the consequences if the truth is discovered. What feared knowledge was President Reagan trying to keep from the American public on Grenada? Why did he bar the press from the invasion of that small island as General Eisenhower did not feel it necessary to do when his forces challenged the might of the Nazis?

There is no great mystery about it, really. Mr. Reagan was afraid that the facts on the ground would not support the reasons he gave for the invasion. He was afraid that public support, as shown in opinion polls, would wither if people learned too much too soon. The official justifications for the attack on Grenada have already started to unravel. What sounded so clear and dramatic in Mr. Reagan's speeches is less convincing in light of facts that have emerged despite the blackout.

The safety of Americans on Grenada was the first reason given by the President in his announcement of the invasion on Oct. 25. He said he had reports that "a large number" were "seeking to escape." U.S. officials said the Grenadian regime had closed its airport. The implication was that the regime was planning to hold Americans there.

Now we know that Grenada and Cuba both sent urgent messages to the United States saying that our citizens, in particular the large number of medical students, were safe. We know that the airport was open and that Americans flew out the day before the invasion, encountering no problems at the airport and seeing not even an armed guard.

The Reagan Administration was in fact not interested in exploring peaceful evacuation of Americans who wanted to leave. It did not look into chartering ships or planes. It did not respond to the Grenadian or Cuban messages until after the invasion was under way. It was determined to make a show of force.

The President did not mention Cuba or the Soviet Union in his original explanation of the invasion. But by the time he addressed the nation on television three nights later, they had dominant and sinister significance. He said Grenada "was a Soviet-Cuban colony being resolved as a major military bastion to export terror."

His statement was no doubt effective politically. It would be hard to find language better calculated to play on American fears than "Soviet-Cuban colony" or "military bastion"

or "terror." But where is the evidence for those terrifying assertions?

Senator Daniel Patrick Moynihan, New York Democrat and vice chairman of the Senate Intelligence Committee, is not exactly soft on communism. After listening to Administration briefings he said: "Nothing has been discovered so far that would show with any certainty that Cuba was planning to take over Grenada."

A Republican senator similarly told reporters: "We need to know a lot more before I'd be willing to accept the assessment that Grenada was about to become a Cuban proxy."

One of the first things reporters will try to find out on Grenada, once they fully slip the leash of Reagan Administration "guided tours," is what the extent of Cuban military facilities was. They will also surely explore how Grenadians feel about the invasion.

The attitude of the Grenadian people is a particularly important unknown, affecting the future of the Reagan operation. The President set as one of his objectives "the restoration of democratic institutions in Grenada." But how exactly is that going to work, politically or militarily? How long will Americans have to stay?

Admiral Vesley L. McDonald, commander in chief of the U.S. Atlantic fleet, told reporters that American troops must get rid of all resisting Grenadian elements before leaving. "We have to identify the people who are the hard-liners," he said. "I think the identification process is going to be one that's very difficult for us to continue to pursue but one that we've got to do because we cannot afford the withdrawal of all of the forces and allow an insurgency government to reappear."

For an outside power to remake the politics of even a small country may be complicated. Did the Reagan Administration think the problem through before taking on the responsibility?

The American people needed light on such questions from the start to enable them to perform their duty of critical judgment on official policy. But Mr. Reagan did not want the inconvenience of democratic judgment. He wanted unrestrained power. Hence his great effort to keep the public in powerless ignorance.

He knew the facts would come out eventually. But if that day could be postponed, it might make a great political difference. People would be left with their first impression that this was a decisive President fighting communism. They would not reckon the cost of what may have been just a hasty, lawless show of muscle.

WASH. POST 10/31/83

Admiral Fights 2 Battles: With Grenada and Press

By Kernan Turner
Associated Press

BRIDGETOWN, Barbados, Oct. 30—The U.S. military commander of the Grenada Task Force is fighting two battles: one with the resistance on the island and another with reporters trying to cover the invasion.

Vice Adm. Joseph Metcalf III says that he has ordered naval patrol boats to shoot at unauthorized small craft attempting to land reporters and photographers on Grenada. Journalists hope that he is joking.

Metcalf, commander of the invasion force, also has rejected complaints from the press about restrictions, saying that he is protecting the reporters' lives by not granting them free access to the island.

Dressed in a beribboned white uniform, Metcalf told reporters at a news conference yesterday to stop trying to take their complaints to a higher authority.

"The buck stops with me," the admiral declared. "If you want to argue with somebody about it, you've got to argue with me, not the DOD [Department of Defense], not anybody else but me."

Earlier in the day, when he was wearing a jump suit and visored cap, Metcalf greeted a pool of reporters in Grenada on a closely guarded visit to the embattled island.

"Any of you guys coming in on press boats?" Metcalf asked. "Well, I know how to stop those press boats. We've been shooting at them. We haven't sunk any yet, but how are we to know who's on them?"

A number of weary correspondents have returned to Bridgetown after hiring boats that were turned back off the coast of Grenada by Navy warships, but there have been no reports of journalists ducking U.S. bullets.

Metcalf, a native of Holyoke, Mass., is a 1951 graduate of the U.S. Naval Academy. He is commander of the Second Fleet.

The admiral's encounters with journalists have revealed a tough, yet good-natured personality. He greets

reporters on the press-pool tours at planeside, shaking hands and asking their names.

But when pressed for specific information, he often says, "I haven't the foggiest idea." He confided to one group of perplexed reporters: "I love that quote."

On some occasions, he has misled reporters. When asked about the capture yesterday of Bernard Coard, the politician who is believed to have provoked the events leading to the slaying of prime minister Maurice Bishop, Metcalf at first told a news conference that Grenadians had detained Coard.

Told that a marine officer had described to the press pool how Coard had been surrounded by marines in a hideout and ordered to come out of the house or be blown up, Metcalf said: "Okay, let's be technical, okay?"

Pressed further by the reporters, Metcalf acknowledged that he was at a Marine command post when Coard was brought in and was aware that the Marines had captured him.

Despite his restrictions, Metcalf insists that he wants "the news media to get on with the legitimate business of public information."

In what appeared to reporters to be contradictory statements, Metcalf accepted full responsibility for keeping reporters out of Grenada despite "enormous pressure in Washington to get reporters in there," and yet called himself the journalists' "best friend."

"I want to get you there but, by golly, I'm going to insist that you can be supported when you get there," the admiral said.

[In a conversation with reporters Edward Cody of The Washington Post and Don Bohning of The Miami Herald last night, Metcalf acknowledged that he deliberately had held them aboard his flagship, the aircraft carrier USS Guam, for 18 hours to prevent them from filing first-hand accounts of the invasion. The task force commander said that he had been "following orders" from Washington in holding the reporters, but he did not specify who had given the orders.]

PRESS CLIPS *The Village Voice*

NOV. 8, 1983

By Alexander Cockburn

The Press and the Invasion

With considerably less resistance than that displayed by the Grenadian militia, important sections of the US media surrendered without much of a struggle in the face of the US invasion of Grenada and the Reagan administration's propaganda barrage to justify this outrageous and illegal venture.

It's true that editorials in the *New York Times*, the *Boston Globe* and the *Washington Post*—to mention three important papers—indignantly denounced the invasion, its legality and its rationales. It's true that an assiduous reader of the papers would have had a fair amount of informative material against which to assess the claims of the administration. But even after last weekend fundamental Reaganite assumptions remained entirely unchallenged in the mainline media.

Keynotes

A crucial moment for the Reagan administration came with the network newscasts on the first Tuesday, the day of the invasion. These, more than any editorial or report in the *New York Times* or *Washington Post*, set the basic terms for public perception. The CBS, NBC and ABC newscasts were all, by and large, ill-informed, if not actively misleading. They accepted most Reaganite assumptions and, particularly in the case of Bill Moyers on CBS, actively endorsed them.

Consider the famous airstrip. For over a quarter of a century the Grenadians have been hoping to lengthen their airstrip, which cannot accommodate the large passenger planes which could bring tourists so necessary to the island's economy. The airstrip has been favorably viewed by the World Bank. At least half its financing comes from western European countries. The British firm of Plessey has been advising on its construction. There is an enormous difference between a civilian airport—which is being built on Grenada—and a military one.

It is not as though such reflections were kept from the highly paid reporters, anchormen and producers who put out the network news. Serious attempts to deflate to sensible proportions the dreaded airstrip were made at the time of Maurice Bishop's visit to the United States this summer. Yet, last week, it is as though such informed assessments had never been made. On CBS, Bob Simon reported jauntily, "The Grenadians said their new all-weather night-and-day airport, with its 10,000-foot runway built by Cubans was for jumbo jets carrying tourists." Washington said, "Nonsense." The Grenadians said the new port facilities under construction were for banana boats. Washington said, "No Way." Washington believed this tiniest Caribbean country was being redesigned from a tourist haven to a Communist airbase and a way station, a stopping-off point for Cuban soldiers on their way to Africa, for East Bloc supplies on their way to Nicaragua.

For ABC, Jack Smith faithfully parroted Reaganite claims about the airstrip and the deep port. NBC was somewhat more restrained. Unchallenged on all three programs was the fundamental premise that Grenada could be of immense military and strategic value to Cuba and the Soviet Union. Why? This was never satisfactorily explained, aside from some astounding boah promulgated by former CIA director Stansfield Turner on *Nightline* to the effect that a Cuban/Soviet controlled Grenada threatened crucial oil-tanker lanes.

Ignorance Is Safe

What is always astounding is that these networks, and indeed these newspapers and newsmagazines, equipped with incredible sums of money and enormous staffs, apparently find it impossible to find anyone who knows anything about the Caribbean, anything about the economy or politics of the region beyond the *New York Post*-size headlines which apparently substitute for thinking inside Reagan's head.

In an entire week, an American citizen would have found it hard to discover that the "democracy" allegedly overthrown by the New Jewel Movement on Grenada was a corrupt and fraudulent regime run by Eric Gairy in which ballot boxes were routinely stuffed, political opponents killed and the economy sold to criminal interests.

Since the press prates on ceaselessly about the public's "right to know," you would have thought that the media would have tried to cater to this same right. Instead of which, on that first crucial Tuesday night, we had this fairly representative slice of nonsense from Jack Smith, ABC news correspondent. Buzz phrases are italicized.

"Former Grenadian prime minister Maurice Bishop, a leftist, recently showed signs of *swinging towards democracy*. He was killed in a bloody coup *et cetera*"—this month and apparently replaced by his deputy, Bernard Coard, a committed ideological Marxist. With Fidel Castro now firmly established as an ally of Nicaragua's leftist regime and with the guerilla war now being fought in El Salvador, the last thing the US or its Caribbean allies wanted was another Soviet or Cuban base, especially since Grenada sits astride the Trinidad channel, which is the preferred route for half of the US's imports enroute to Gulf Coast refineries. Today's events recall a similar crisis, 18 years ago, when US troops intervened against leftist rebels in the Dominican Republic. That intervention is now largely forgotten and the Dominican Republic a democracy. It remains to be seen if today's action will turn out as well. Jack Smith, ABC News, Washington."

But if you think this is bad, try Bill Moyers's revolting homily:

"In a world where freedom has enemies, the use of force can be justified. The question is always when and where. . . . You can argue that a tiny island with a leftist government could scarcely have been more than a nuisance, if that. But then that huge airstrip appeared, built with Soviet and Cuban help, and harder-line Marxists trained in Cuba threw out the hard-liners already in power. There followed a blood letting *et cetera* to the one Marxist had already inflicted on opponents in nearby Surinam.

"You can hardly blame the peaceful islands around Grenada for being alarmed, or an American president for imagining the strategic consequences, of yet another Soviet base in the Caribbean. John Kennedy almost went to war to get Soviet missiles out of Cuba; and Lyndon Johnson sent some 20,000 troops, of whom 28 died, to prevent a Communist takeover in the Dominican Republic. So it's not surprising that Mr. Reagan would also consider the use of force legitimate in the Caribbean.

"Whether the price was worth it depends on whether the result is to replace their 'things'—as Mr. Reagan calls them—with our thugs, as happened in Guatemala, in Chile—Chile, or whether the people of Grenada really get their freedom. If this happens, there will be no less grief for the next of kin of the troops who died in Grenada than for those down in Beirut; but at least they can say, 'mission accomplished.'"

Brainwashing Techniques

Notice, *inter alia*, the mechanical repetition "trained in Cuba" as a way of categorizing opponents of the US. The technique—which has nothing to do with truth, since neither Bishop, Coard or for that matter Austin were "trained" in Cuba—is kindred to the Israelis' systematic use of "terrorists" for Palestinians. Persistent use of "Cuban-trained" or "Cuban presence" or "Cuban support" gradually induces a pathological response, in other words, brainwashing.

Note above all the distortion of Lyndon Johnson's intervention in the Dominican Republic, for which Moyers may indeed have had a soft spot since he was in the White House working for Johnson at the time.

Johnson used the excuse of a threat to Peace Corps volunteers in the Dominican Republic to try to prevent not a Communist takeover but the overthrow of a rightist junta by a group of nationalist junior officers with a reformist bent. The Peace Corps volunteers met later to prevent LBJ's use of them as a rationale for intervention with 21,000 marines, which tells you the difference between 1965 and 1963, with those medical students slobbering over US soil after being rescued by marines from the consequences of a US attack.

Notice finally that none of these law-abiding commentators actually care a fig for the law. Not Moyers, who simply says that the end can justify the means and hang the consequences, nor James Reston who said the same thing. I exclude here such predictable desperados and ardent supporters of the Reagan administration as Norman Podhoretz ("Grenada points the way back to recovery and health") or the *Wall Street Journal* editorial page, which declared exultantly that the world was the better for this display of US military might.

The media had some problems with the first of the Reagan administration's excuses for intervention—the "appeal" from the Organization of Eastern Caribbean States. The flouting of the UN and OAS charters, not to mention the famous section 8 of the OECS charter, was too blatant. But even so, you had to read long and hard to discover that the US almost certainly backdated the so-called appeal for intervention of Governor General Sir Paul Scoon and in effect kidnapped him onto the USS *Gunn*—where legally he had no standing as governor general, since he was not on Grenadian soil.

After a brief moment in which Dr Modica, representative of the St George's medical school in New York, maintained that intervention was unnecessary and might indeed endanger the students, the press collapsed, along with Modica, and accepted the Reagan line. Amid the emotional pictures of students kissing US soil, few pointed out that they were escaping from danger provoked by the US attack.

My colleague Jason Salzman talked on Monday to Alice Palatnick, who had just got back from Grenada where she had been visiting a friend in the medical school. Palatnick says she felt in no danger during the curfew period. "Half the med students didn't like the Grenadians. Students called them FICS—'Fucking Ignorant Grenadians'. This is indicative of their attitude, especially the ones who came back and who were kissing the ground. . . . From Tuesday to Friday when we were hit out we just viewed the war. The only time I felt endangered was when the Americans bombed nearby. Jim Hochstetler, a med student who lived in the area, had his house totally destroyed by a bomb on Tuesday. The whole time I was there not once did I hear of Grenadians or Cubans attacking any students. The attack put us in incredible danger because the Americans did not know where we were the first days. It was thanks to the good will of the Cubans and Grenadians that I didn't get hurt. The American soldiers didn't even have maps to the island. They borrowed all our maps and blueprints."

With the US military's censorship, which produces howls of outrage, the story turned into a rather self-regarding saga of how the US press tried to invade Grenada on its own. Of course the censorship did have a purpose which the press, amid all its indignation, did not point out—perhaps because the networks were too busy running DoD film and the editor of *Newsweek*, Maynard Parker, too occupied denouncing his photographer, who let the side down by breaching army rules and staying beyond his appointed term. The point was that the US invading force was hoisting down Grenada with 20-millimeter rounds from its AC-130 gunships, in salvoes which, if Vietnam is anything to go by, produced large numbers of civilian casualties. Simultaneously, artillery salvoes were leveling such institutions as the mental hospital, as Paul McLane in this paper and others have described. The *New York Post* was decent enough to call this one of the "misfortunes" of war. So it was, but one can imagine what the *Post* would have said if some force other than the Americans had been responsible? The "accident" would speedily have become a war crime.

By now the Reagan administration had cast aside the student/postage rationale and was claiming that it had got there "just in time" to prevent the conversion of Grenada into a Communist version of Guantanamo. Once again, before journalists such as Loren Jenkins of the *Washington Post* actually took a look at the famous warehouses with their venerable guns and the Cubans provided full lists of their people on the island, the networks and papers bought the story.

"American military sources say they were staggered by the depth and strength of the Cuban military presence," ABC's John McWethy reported on Thursday night. He went on to speak of our old friend "sophisticated communications equipment" and "what one intelligence source described as an enormous supply of ammunition and weapons". This all turned out to be lies of course, but by then the damage, or rather the good—if you look at it from the Reagan administration's point of view—had been done.

Very late on Thursday night, too late for the Friday morning headlines, the US ended up isolated in a Security Council vote—a solitude reminiscent of French and British isolation in the wake of Suez. But US media, which could hardly keep out of the Security Council for an instant when it was a matter of condemning the USSR for KAL 007, had far less to say on this occasion.

It's not that there was no decent reporting at all, though television was by and large disgraceful. It's more that the Big Lie techniques of the Reagan administration, now in full and menacing flower after three years' growth, overwhelms conventional journalistic techniques with sheer volume of arrogant mendacity. In one of the few really tough pieces, Robert Kaiser pointed this out in the *Washington Post Outlook* section last Sunday:

"But if the limitations of Reagan and his team are widely accepted by the expert community in Washington, the experts mostly keep still. Reporters who also realize that many officials in this administration are less than wise don't know how to put that into print. . . . Lou Cannon, the *Post's* White House correspondent, wrote the other day that according to a congressman who heard him discuss the invasion of Grenada, Reagan displayed 'an unusually detailed grasp' of the issues involved. A reader from Miami might have thought that this meant that in absolute terms Reagan had a splendid mastery of the material. But every insider in Washington knew what Cannon was talking about was intended—that this time, Reagan knew something about what he was discussing."

"Everybody in this town has known that the emperor has no clothes," said the same former cabinet member. "But there has been a polite silence not to say so." Politics or football? Perhaps, once again, the American people will have cause to complain that the establishment that is supposed to know the most about these things failed to warn its countrymen of the danger it faced. If the people who know most say nothing, what is the good of having the freedom to speak out?"

Essay

Trying to Censor Reality

The wisdom of the U.S. invasion of Grenada will be debated for years. The unprecedented exclusion of the American press from that operation requires no debate; clearly it was a bad mistake, an outrage to press freedom and an ominous symptom of a tendency in the Reagan Administration to try to control the flow of information.

All Administrations attempt to do this, up to a point. Actually the Reagan White House has been far more intelligent and helpful in its dealings with the press than was customary during the Nixon age of paranoia and the Carter era of petty meanness. Thus the attempt to fight a little war in secret, out of range of reporters and cameramen, is all the more startling and unfortunate.

The explanations offered by the Administration were preposterous. Secretary of Defense Caspar Weinberger argued that the armed forces could not have guaranteed the safety of journalists. But American journalists have never demanded such guarantees.

They have worked and died in the Civil War, World War I, on the beaches of Normandy and Okinawa, in Seoul and Saigon. Weinberger's other reason, that the commander in the field did not want the press along, was a glaring cop-out. No question was raised about press coverage aiding the enemy; that was wise. The press invariably accepts ground rules on matters of true security, where lives and operations are at stake.

Why should anyone care about this? Many people might assume that the press was protesting against its exclusion out of a prurient or even commercial itch, annoyed at missing some sensational headlines and pictures. That is simply not the case. The press has a serious quasi-constitutional function as a representative of the public. Obviously the White House or the Pentagon remembered the Viet Nam "living-room war" and the revulsion it created. Obviously they admired and envied Margaret Thatcher's dealing with the press during the Falklands invasion, when the Iron Lady's government allowed only a small contingent of journalists along, under wraps.

It was quickly apparent that banning reporters—and later giving them only a few quick guided tours—hurt the Administration itself. Whenever the press is excluded, speculation and rumor take over. Several days after the invasion there was still determined resistance here and there, but no one knew how much, how serious or by whom. The result was vague and nagging alarm, a suspicion that the world's largest military power had trouble subduing a flyspeck island. However that impression might be dispelled later, some of the damage will linger. More important, the Administration's case for the invasion rests increasingly on the assertion that the Cubans had been attempting to transform Grenada into a sort of island fortress. Eyewitness reports from correspondents might have made that claim quickly convincing. Their absence may cause the question to persist: What was the Administration trying to hide?

Certainly the press has no corner on virtue—far from it. Journalists exaggerate, misunderstand, mislead. They can be irresponsible in big ways and in small. It is hard to forgive those television reporters who, after the Beirut attack, intruded on anxious families with fituous and cruel questions like "How would you feel if your son were among the dead?" On a larger scale, it can be argued that ever since Watergate much of the press has been too automatically hostile toward government.

But freedom of the press, like all freedom, has its risks. It cannot apply only to journalists who are always responsible or posi-

tive. Such freedom would not be freedom at all. On balance, for all their doubts about the press, Americans have usually felt that it represented a pretty good bargain: the occasional outrageous or merely irritating lapse is an acceptable price for journalism's role as witness and watchdog.

Secrecy is addictive. Perhaps the greatest danger in the banning of the press from the Grenada operation is that the Administration will try to repeat it in other situations. The Grenada ban is not an isolated incident, but part of a pattern. Members of the Reagan Administration try not only to control the news and the "image" of its doings but also to shape a whole climate of opinion. The Administration has been active in excluding foreign speakers deemed dangerous or subversive. It has tried to discredit as propaganda fairly innocuous foreign films, and it has fought sharply to limit the Freedom of Information Act. To plug leaks, it has made an estimated 2.5 million federal employees subject to random lie detector tests.

Reagan also has moved to establish sweeping new rules requiring senior Government employees with access to highly classified information to submit any writings—books, articles, letters, speech drafts—for advance Government clearance if there is any possibility that they allude to sensitive activities. This rule, temporarily stalled in the Senate, would apply to these Government employees for their entire lifetime. Had it been in force in the past, it would have required previous clearance and presumably endless battles with censors by writers ranging from Grover Cleveland to George Marshall to Henry Kissinger.

There is no denying that the Government must be able to do certain things in secret. Diplomacy is one of them. So are covert activities, in which all nations, democratic or otherwise, engage. Arguably the threat on Grenada should have been handled by the CIA rather than by the Marines and paratroopers—except that for years now, the CIA has been unable to do anything much without almost instant publicity. But the fault for this absurd situation lies more with Congress and Government officials than with the press. It is also true that the Freedom of Information Act has been abused. But taken together, the Administration's measures suggest a certain mind-set: the notion that events can be shaped by shaping their presentation, that truth should be a controlled substance.

All of this does a real disservice to Ronald Reagan. In many ways he is the most open President we have had in a long time. It is hard to question his sincerity. When he speaks, he radiates conviction. He is attempting to do something important about America's position in the world, to restore its strength and self-respect. One can question specific acts and policies, but the overall goal is urgent and valid. That goal, however, is jeopardized by misperception of what the world is really like, what works and what does not work. The left-wing liberals have been the master illusionists for years, and their image of the world is as mistaken as any right-wing ideologue's. Reagan has a real opportunity to tear between the wishful thinking of the doves and the vengeful daydreams of the hawks, to introduce more realism into American foreign policy. In fact, he has shown signs of doing precisely that in recent months. The crude attempt by bureaucrats in and out of uniform to censor reality, to manage not only news but history, undermines that realistic trend. It also undercuts the trust the country still has in Reagan himself.

—By *Steve Cooney*



U.S. Press Curbs in Grenada May Affect International Debate

By JOSHATHAN FRIENDLY

Some American reporters and press organizations say the Reagan Administration's restrictions on the press in covering the invasion of Grenada may damage Washington's position in a continuing international debate over controls on the gathering and dissemination of news.

Western news organizations and most Western countries, including the United States, have been fighting proposals for press controls proposed by the Soviet Union and many developing countries. Those proposals, advanced in the last decade in forums of the United Nations Educational, Scientific and Cultural Organization, include giving governments a right to force the press to report positively about government actions and licensing journalists as a way to protect them in war zones.

It is now broadly criticized by press groups, the Defense Department barred reporters from covering the first two days of fighting in Grenada and then provided limited guided tours of some parts of the island for two more days. The Pentagon said the limitations were initially needed to prevent advance disclosure of the operation and were later retained because the military could not assure the safety of correspondents.

On Sunday, the man who approved the news restrictions, Gen. John W. Vessey Jr., chairman of the Joint Chiefs of Staff, said he would create a panel of officers and journalists to review the restrictions in the first days of the invasion.

Unesco Conference in Paris

Leonard R. Sussman, executive director of Freedom House, a New York organization that has fought against press restrictions, said he anticipated the news controls in Grenada would be cited this week at the Unesco conference in Paris. Mr. Sussman is a member of the United States delegation to that meeting, which is scheduled to discuss a range of communications proposals, including a Soviet resolution that among other things affirms the right of governments to control some kinds of news.

An official in the State Department's Office of Communications and Unesco Affairs said the delegation to the Paris meeting had been instructed on the Grenada news-control question because "it is likely some mention will be made" of the issue. He declined to say what the instructions were.

Mr. Sussman said that although he thought the controls were wrong, he intended to respond to any criticism by noting that the controls were less re-

strictive than those routinely imposed by other nations and that they were finally lifted after an "upsurge in the press of the kind that only happens in a free society." He said the issue would be raised "more as a matter of rhetoric by countries that are year-round censorers themselves."

*Prejudices the Position

Seymour Topping, managing editor of The New York Times, said, "The extraordinary restriction imposed on the press in the coverage of the Grenada invasion prejudices the position the United States has taken in international forums on freedom of the press." Mr. Topping is chairman of the international communications committee of the American Society of Newspaper Editors, which, like other press groups, protested the controls.

He said the Western arguments to be made in Paris "inevitably will suffer as a consequence of the example set by the Defense Department in denying access to correspondents in the coverage of the Grenada operation."

"We cannot effectively preach freedom of the press abroad unless we practice it at home," Mr. Topping said.

Resistance to Informing Order

The Reagan Administration, like its predecessors, has resisted the "new

world information order" that has repeatedly been proposed by third-world and Soviet bloc nations in Unesco meetings. By coincidence, on the first day American marines landed in Grenada, Mr. Reagan repeated his stand that "accurate, objective information is necessary to the preservation of democracy and freedom."

In a message congratulating the Foreign Press Association on its 65th anniversary, Mr. Reagan noted his opposition to "restrictions on the right of journalists to report events and information as they see fit, free of authoritarian restrictions and official or ideological guidelines."

Journalists were particularly critical of the Defense Department's reasoning, that reporters should not be allowed in Grenada until their safety could be assured. Unesco has debated the issue of identification cards to journalists as a way to protect them in combat zones, but the Western press has said, as it did in Grenada, that reporters are responsible for their own security and that the proposed cards could easily turn into a system for governmental licensing of journalists.

An Insult, Publisher Says

R. M. White 2d, publisher of The Mexico (Mo.) Ledger and chairman of the American Committee of the Inter-

national Press Institute, said the idea of protecting journalists was an insult to the memory of war correspondents killed "so that the American public could have an accurate accounting" of the progress of fighting.

Dana R. Bullen, executive director of the World Press Freedom Committee, based in Washington, said the Grenada curbs "are bad whether its our Government or Zimbabwe."

The restrictions surprised the Western press because in other situations the press has had almost total free access to scenes of fighting. In the battles around Beirut, for example, American correspondents have been able to reach both sides. Some reporters interviewed Druse militiamen under fire from American warships.

In Grenada, however, almost all foreign reporters were expelled after Prime Minister Maurice Bishop was overthrown a week before the invasion.

Dwight Whyllie, a Canadian Broadcasting Corporation reporter, filed reports until he was expelled the day before the invasion. He was in St. George's helping train the staff of the Government-run Radio Free Grenada under a program sponsored by Unesco.

Look for Science Times on Tuesday

NYT

11-8-83 p. A10

RICHARD COHEN

HEY!

Hey there! I'm talking to you. I'm talking to those of you who have not paid any attention to what has been going on between the government and the press, who either think that the press had it coming or that this is just a fight between big government and big media and has nothing to do with you. Wrong. It has only to do with you.

I am referring, of course, to the government's attempts to first keep the invasion of Grenada a secret and then later to obstruct the reporting of it. The first is no big deal. The government is entitled to keep a secret or two, especially if the purpose is to save lives.

As for the second, it is a different matter entirely. The reason the government deterred reporters from filing stories, the reason it made the entire island off-base to journalists and then opened it up only on a selective basis, had nothing to do with the media. It had to do with you—the people who either read or watch the news.

It had to do with the fact that the government did not trust you to come to the right conclusion. It thought certain facts would only turn your little heads. This is the ultimate example of the government playing nanny, and deciding, for your own good, of course, that there is certain information you should not have.

The immediate genesis of this policy is the experience of Vietnam. Many critics of the press, especially on the political right, believe that it was the press, not the Vietnamese, who beat the American military in Vietnam. What the communists could not do with bullets, the press accomplished by demoralizing the homefront. This is a neat little theory, laid out in all its absurdity in the

current issue of the neo-conservative journal, *The Public Interest*. It merely overlooks 50,000 dead, illogical war aims, and a corrupt regime in Saigon.

The same sort of thinking has been applied by the same sort of people to the Israeli invasion of Lebanon. That, too, could have been a success had it not been for unseemly newspaper and television reporting—all of it emphasizing civilian casualties at the expense of the military and political goals of the invasion. Thus, once again, a glorious and wonderful war was spoiled by a press that emphasized the sensational at the expense of the prosaic—the fact that Israel was doing the dirty, but the necessary.

There is something to all this, of course. No one would deny that the picture of the child burned by napalm is a lot more gripping than a dryly written policy paper on why the napalm had to be dropped in the first place. And it is true that all wars, even just ones, entail suffering and horror—much of it visited upon the innocent.

But it is also true that the two wars cited—Vietnam and Lebanon—were fought in the wrong place at the wrong time and for the wrong reasons and that both governments had ample opportunity to make their cases. Both governments, having done that, lost the debate. Either domestic or world opinion reached different conclusions. The way around that, of course, is to silence one side of the debate.

This is what was effectively done in Grenada. The government made sure that the public would not have its head turned by the usual pictures of carnage. And it succeeded. For the first time in a long time, we fought a war that resulted—at least where television was concerned—in no dead, no suffering, no civilian casualties. It was a most lovely war. But it was hardly the whole truth.

This management of the news is practiced in countries where the people are not trusted to come to the right decision. It is standard practice in Third World and communist countries where there is no concept of truth—just information that's helpful and information that's not. The latter is proscribed—always in the name of the people and always for the good of the people.

That's why I'm talking to you. You're wrong if you think this flap between the press and the government is none of your business. It is your business because it is not about the press at all, but about you. It's the press the government blames. Because it's you it fears.

Information Blackout Revives Old Issues

By David Margulies
Washington Post Staff Writer

The U.S. military had just completed a high-stakes operation in the Caribbean. During its crucial early days no American journalists were allowed near the action.

"Do not talk to me about what we will lose; we already have lost," a defense industry journalist said. "A dramatic chapter in history has gone unrecorded by objective newsmen because this administration chose a course that never was undertaken in the Civil War, World War I, World War II and Korea. It kept reporters out of the action. This is an act of shame."

Many considered the news media blackout part of a widespread and in some respects unprecedented peacetime effort by the government to manipulate the news and stifle the free flow of information. In one year alone, polygraph operators administered 18,122 lie-detector tests to federal employees for security clearance and investigations of security leaks. Defense Department workers were instructed to report to their superiors every contact they had with the press. Pentagon spokesmen said they had a duty to manipulate some information as a weapon against communist enemies. One said the government had, under some circumstances, an inherent and basic right to lie to the public.

All this happened two decades ago during the Kennedy administration, beginning with the Cuban missile crisis. Today, in the aftermath of the Reagan administration's invasion of Grenada, the conflict between government information control and the media's assertion of the public right to know is strikingly familiar.

Again a decision to keep reporters and cameramen away from an unfolding military operation in the Caribbean provoked condemnation from the news media. Once again it was linked to what some perceive as a widespread and systematic attempt by the executive branch to control and manipulate the flow of information.

In the cause of making America secure against public disclosure of sensitive information, the Reagan administration has imposed new orders making it easier to classify more documents as secret and to keep more unclassified documents out of reach of the Freedom of Information Act. It has instructed all employees who deal with intelligence matters to get approval from senior officials before talking with the press.

It has issued directives, temporarily stalled by Congress, requiring 112,000 federal officials with security clearance to submit to lie-detector tests if asked and to sign contracts making anything they ever write about government intelligence subject to prepublication review and censorship. It has prevented university scientists in several high-technology fields from releasing papers on their unclassified research and from associating freely with colleagues from Marxist countries.

"It is a pattern of activities," said Bruce W. Sanford, a prominent First Amendment lawyer in Washington, "that has given the Reagan administration, easily the worst record of any modern presidency on the issue of openness in government."

When asked to report to such changes, administration officials tended not to rebut them directly, but rather challenged the premises

that the free flow of information in government is inherently good.

"We went through a period where we were seeing more and more openness in government. And we think it went too far," said Richard K. Willard, the deputy assistant attorney general who drafted several of the administration's new directives.

"Certainly there was great disillusionment about the government's national security apparatus in connection with Vietnam and Watergate, and this concern produced some good reforms, but also some serious problems. There arose a dangerous degree of laxity about real security concerns."

When asked by a Los Angeles Times reporter about the press blackout on Grenada, White House chief of staff James A. Baker III said that "a large majority of the American people support it." A Pentagon spokesman said essentially the same thing in sharper words when responding to a query from a Washington Post reporter: "I guess most of the people think I don't have to tell you a damn thing."

"A startling lesson of the Grenada invasion episode is that the news media, arguing the public's right to know, found themselves without general public support," said Cable News Network's Daniel Schorr, who noted that four-fifths of the respondents to his network's call-in shows supported Pentagon restrictions on Grenada news coverage.

The findings of a Washington Post/ABC News poll conducted Nov. 3-7 revealed something quite different, however. It asked, "Would you say the U.S. government has tried to

control news reports out of Grenada more than it should, or not?"

Nearly half—46 percent—of 1,505 respondents nationwide said yes, that government had tried to control reports more than it should have, 38 percent said no and 15 percent had no opinion. A sociological and demographic breakdown of every response indicated that every grouping except two—Republicans and persons over age 45—thought the government controlled the news coverage from Grenada too much.

The poll was conducted more than a week after the Oct. 25 invasion, during a period when government officials were revising and in some cases retracting early reports on, among other things, the number of Cubans on the island, the resistance American forces met from Grenadians, the casualty estimates and the ability of American students to leave Grenada the day before the invasion.

There were two elements to the Reagan administration's explanation for keeping the news media out of Grenada during the early fighting: it was a military decision, not a civilian one, and it was based on safety concerns.

"The reason is of course the commander's decision, and I certainly don't ever, wouldn't ever, dream of overriding commanders' decisions in charge of an operation like this," Defense Secretary Caspar W. Weinberger said. "Their conclusion was that

they were not able to guarantee any kind of safety to anyone, including of course anybody participating, and that you have to maintain some kind of awareness of the problems going into areas where we don't know what kind of conditions totally will be encountered.

"The airport was obviously heavily overclouded with all kinds of activity and we just didn't have the conditions under which we thought we would be able to detach enough people to protect all the newsmen, cameramen, gripemen, all of that."

His explanation struck several former Pentagon officials as illogical.

"Senior government officials must remember that for years professional journalists and professional public officials have been able to find ways to provide both troop security and the flow of information which an open society demands," said Jerry W. Friedheim, the assistant secretary of defense for public affairs during the most contentious days of the Vietnam war.

Friedheim, who now serves as executive vice president of the American Newspaper Publishers Association, added: "One need only recall the actions of Gen. Creighton Abrams in personally assuring press access to his troops during the troubled days when controversial combat actions were under way across the South Vietnam border in Cambodia. Gen. Abrams understood that he and his troops were working within and for a constitutional, free society. He saw it as his duty to help a free press serve a free society. He was right. Today's officials are wrong."

Another former public affairs official in the Defense Department

during the Vietnam era, Daniel Z. Hamkin, questioned the wisdom of leaving such a decision entirely in the hands of the military.

"I think in our form of government there is a responsibility that civilians participate in such decisions," he said. "And I do have the sense that, if not with the initial landing, there were ways that could have been devised to handle the press very early on."

One White House official said the top military brass, including Gen. John W. Vessey Jr., chairman of the Joint Chiefs of Staff, held the view that "if you get the news people into this you lose support of public opinion."

Throughout his years in public life President Reagan has shown absolute respect for institutions of au-

thority. This was the case when he was governor of California and the police battled students on the University of California campus at Berkeley, and has held true during his presidency with the military and intelligence agencies. One of his self-proclaimed missions has been to reverse what he has called the "Vietnam syndrome," a lack of confidence in the armed forces and the CIA.

In a March, 1983, interview in TV Guide, Reagan criticized the media for covering the Vietnam war from the perspective "that the war was wrong. Had that been done in World War II, in behalf of the country that was killing American military men, I think there would have been a revolution in America."

Reagan similarly criticized media coverage of the American role in El

Salvador. "There has been a kind of editorial slant that has something, almost, of the Vietnam syndrome, which challenges what we're doing there," he said. "I could say to the press, 'Look, I will trust you to believe you what we're trying to accomplish. If you use that story, it will result in harm to our nation, and probably make it impossible to do what we're trying to do.' But they just go with the story."

It is from this perspective that Reagan, from the first days of his administration, has been consumed by efforts to keep what he considers to be sensitive information from being leached to the media and disseminated to the public. There is a long and rich history of presidents being upset about news leaks and uttering variations of Reagan's "up to my bustle" lament.

There also is an equally long tradition, carried forward in the Reagan White House, of senior officials publicly embracing their president's efforts to control leaks while slipping selected information to the reporters of their choice. Only recently, for example, one mid-level official was lectured sternly by one of Reagan's senior aides for leaking information. When his knowledge was white and he expected to be fired, the others broke into laughter and told him not to worry, they do it all the time.

But many in the media and the law who serve as watchdogs of the public's right to know assert that never before has an administration made such a sustained and multidimensional effort to restrict the flow of information.

"There is a very major Big Brother complex in the Reagan administration. We know best—that seems to be the underlying theme," said John Munn, a former congressman



A photo sent from Berkeley appears to show a reporter standing near a vehicle at night before the Oct. 20 closing of Police Minister Marko Ruppel. It was used in the AP by an agent for a photographer requesting comment.

**"ISN'T THIS BETTER THAN ALL THOSE NEWS
STORIES YOU GET FROM THE PRESS?"**



Post Dec. 16, 1983

Hints at Future News Blackouts Shultz Defends Press Ban

By Margaret Shapiro
Washington Post Staff Writer

Secretary of State George P. Shultz yesterday said that journalists were barred from covering the invasion of Grenada because "reporters are always against us and so they're always seeking to report something that's going to screw things up."

Shultz also said it was possible that reporters would be banned from other military actions in the future because the priority in such cases will be on accomplishing a mission and "not blowing the operation by this tremendous sense that reporters seem to have these days that they have to know everything before you do."

Shultz's comments were made during an interview Wednesday with editors of the Connecticut newspaper chain. When asked about the decision to bar reporters from Grenada during the Oct. 25 invasion and overturn a tradition that has been in place for several U.S.

wars, including World War II, Shultz replied: "Then, reporters were involved all along. And on the whole they were on our side."

"These days, in the adversary journalism that's been developed, it seems as though the reporters are always against us and so they're always seeking to report something that's going to screw things up. And when you're trying to conduct a military operation you don't need that."

After making this statement, Shultz softened it somewhat, acknowledging that "I've kind of gone around the barn a little bit on your question" and adding that he believes that a free press is vital to a free society.

Later, when the editors asked President Reagan a similar question, he said logistical questions were left to the military, and that there was "no conscious decision by anyone" at the White House or State Department to bar the press from the Grenada landing.



GEORGE P. SHULTZ

... "reporters are always against us"

White House spokesman Larry Speakes yesterday tried to put some distance between Shultz's statements and the White House.

"I do not think that reflects the attitude of the president or the senior staff of the White House," he said.

sam. 12/16/83
Role of the Press

Q. Mr. President, on the press, Secretary Shultz said the other day that in World War II reporters went along because, on the whole, they were on our side. And then he observed that these days it always seems that the reporters are always against us and they're trying to report things to screw things up. Is that your view of the press, also?

A. Now you're not going to get me into the middle of that, are you? I'm simply going to say that I do believe, Sam, that sometimes, beginning with the Korean conflict and certainly in the Vietnam conflict, there was more criticizing of our own forces and what we were trying to do, to the point that it didn't seem that there was much criticism being leveled on the enemy. And sometimes I just wish that we could get together on what is of importance to our national security in a situation of that kind, what is endangering our forces and what is helping them in their mission.

Q. Well, sir, is one of the problems a definition of the word "us"? When Secretary Shultz uses it, or if you say "our forces," do you think he was using it in terms of an Administration, the Reagan Administration?

A. No.

Q. Or, let's say, the Carter Administration? In other words, is "us" the Administration in power, or is there a higher duty that the press has?

A. I thought the us he was talking about was our side, militarily -- in other words, all of America.

You -- Allred.

Media Curbed Out of Dislike, Admiral Says

CORONADO, Calif., Dec. 15 (UPI)—The admiral in charge of the Grenada invasion said reporters were left behind partly because many of his fellow officers harbored a strong dislike of the media.

Vice Adm. Joseph Metcalf told the San Diego Tribune that he would have allowed a party of eight journalists to accompany the invasion fleet, but did not want to deal with a press corps numbering in the hundreds.

"I didn't want the press around where I would start second-guessing what I was doing relative to the press," said Metcalf, who addressed a group of Naval Academy graduates at the Naval Amphibious Base at Coronado.

"We think there is a lot of resentment of the press in the Navy, but that's minor compared to the Army and Marine Corps," he said, adding that both commanders and journalists must reconcile their differences.

Sunday, January 29, 1984

THE WASHINGTON POST

Haynes Johnson

ECHOES

Notes on the aftermath of the media and Grenada: another national Harris opinion survey offers polling evidence that Americans have not deserted the media on the right to cover news. It also shows that citizens back the media over the government on coverage of the Grenada invasion. By 65 to 32 percent, those polled said they believed that reporters should have been allowed to accompany U.S. troops invading Grenada.

At the time of the Reagan administration's ban on coverage of that invasion in October, this column dealt at length with the overwhelmingly negative view of American media performance in general and support for the government's position on the media in Grenada specifically as reflected in a massive stream of letters from around the country. Those letters continued to arrive for weeks. Since Harris' data now indicate that public attitudes are different than I reported, or that they have changed, I am happy to add his figures for the record on the subject.

Some of his other findings: by 53 to 36 percent, those polled think that the country was better off because Vietnam was fully and graphically covered. Eighty-three percent agree that, in a free country, a basic freedom is the right to know about important events, especially where the lives of American soldiers are concerned. By 63 to 34 percent, they agree that by not allowing at least a small pool of reporters to report an invasion, a president or the military might be tempted to cover up mistakes and lives lost. And 52 percent disagree that the press and television pry too much into too many things as it is.

Harris concludes that those who raised questions about harsh anti-media sentiments in the country were wrong. Let us hope so, but on this subject I remain from Missouri. I have to be shown further that public attitudes about the media are still not strongly negative.

"Barring Reporters from the Battlefield"

By Drew Middleton

MILITARY TEXTBOOKS OF THE future will probably cite the United States invasion of Grenada as a swift and effective operation carried out with minimal casualties and the accomplishment of major objectives. But the textbooks, being military, will probably omit one unfortunate consequence of the operation — the worsening of relations between the news media and the military resulting from extraordinary restrictions placed on the former by the latter.

The significance of this deterioration lies as much in its carry-over effect as in the immediate impact. The increasing number of global flash points, such as Lebanon, the Persian Gulf, South Korea and Central America, seems to insure that other American military operations will soon provide new testing grounds. How both sides meet the challenges to come will have a profound effect on a relationship of great importance not just to the parties involved but to the American public as a whole.

The decision to deny access to press, radio and television reporters during the early stages of last October's operation in Grenada ran against the course not only of military precedent but of a history of considerable media freedom in covering American military conflicts that dates back to the Civil War. Although the armed forces had frequently raised objections and barriers, often for reasons of security, there had, on the whole, been a balance, with the military benefiting as much as the media. The exception was the Vietnam War, the final years of which were the nadir of media-military relationships.

There is little doubt in the minds of experienced observers that post-Vietnam military attitudes influenced the decision to shut the media out of the landing in Grenada and of the earliest mop-up operations. The majors and commanders of the Vietnam War who believed the media had worked against the American command there had become influential generals and admirals determined not to expose the Grenada operation to what they continue to view as a hostile adversary. That attitude was reflected by President Reagan during a December press conference when he said that in Vietnam the press was not on "our side, militarily."

The media track record has, in fact, been creditable. In Vietnam, as in earlier wars, members of the press proved their ability to preserve the security of military actions and landings. And they have routinely exposed themselves to danger while covering conflicts involving American troops, including at present the action in Lebanon.

Their interest in continuing to do so was expressed strongly in January when 10 major news organizations issued a joint statement calling on the Reagan Administration to affirm the right of journalists to cover United States military operations. Leaders of the news groups indicated they could agree on limited restrictions, such as delayed filing and military censorship, so long as reporters were not excluded from combat missions and thus denied the right of independent reporting. The White House said it was trying to arrange a meeting with the group's leaders, and the Defense Depart-

ment announced that the Joint Chiefs of Staff were creating a special panel to study the issue, with hearings to begin sometime in February, in which the organizations issuing the statement have said they would voluntarily participate.

THE CIVIL WAR, THE GREATEST CONFLICT ever fought on this continent, marked the emergence of the American war correspondent. The writers and artists who covered the war between the states enjoyed extraordinary freedom. Many of them passed easily from one side to the other. By modern stand-

ards, their accounts were less than objective and, in many cases, unduly prepared to accept the military's version of the situation. For instance, despite the example before them of the disclosure of medical breakdown in the Crimea by *The Times* of London's correspondent William Howard Russell, the horrors of military hospitals and prisoner of war camps received scant attention at the time.

Even so, reporters earned the enmity of some top soldiers on the Union side. Gen. William Tecumseh Sherman, who led the North's march through Georgia to the sea, complained of correspondents "picking up dropped expressions, inciting jealousy and discontent and doing infinite mischief."

Relations improved during the Indian Wars that occupied the Army for a third of a century after the South's surrender at Appomattox, largely because there were so few reporters on the spot. But correspondents did ride with Gen. George A. Custer and Gen. George Crook, and they subscribed, in the main, to the then-popular doctrine that the only good Indian was a dead Indian.

Relations deteriorated during the Spanish-American War. Maj. Gen. William B. Shafter, commander of American troops in Cuba, had little use for reporters, including the famous correspondent, Richard Harding Davis, who stridently supported the Government's position in *The New York Journal*. It was left to Lieut. Col. Theodore Roosevelt, who had his eyes on summits beyond San Juan Hill, to coax the press and leave the reading public with the impression that "Teddy" had won the war.

The American Army entering World War I found itself wrapped in the censorship already established by Britain and France, the senior allies, who instituted it for purposes of security. There is little doubt but that Gen. John J. Pershing, the commander of the American Expeditionary Force, found the restrictions congenial. Before the First World War I began, having persuaded the War Department to keep the press away during his pacification of Mindoro Island in the Philippines, Pershing had managed to fight a successful campaign without any media scrutiny.



Reporters assigned to the A.E.F., like those assigned to the British and French forces, had a certain freedom of movement but a thin diet of news. What they did write was largely favorable to the Allies. But because of the censorship, neither they nor their allied colleagues reported one of the major events: the French Army mutiny in 1917.

By the time World War II came along, the British had learned a lot about the uses, and usefulness, of censorship. To a people fighting for their lives, as the British did following the defeat of the French and before the Americans entered the fray, censorship was an acceptable if not particularly attractive practice. With his feel for the (Continued on Page 61)

ears mind, Prime Minister Winston S. Churchill understood, however, that if all the bad news was concealed through censorship, the British public would come to doubt everything the Government said. So although a great deal continued to be censored — tonnage of ships sunk, the exact extent of air-raid damage — a good deal more was written about than would be deemed prudent today by President Reagan.

Although a gap existed between the media and military during World War II, there were reasons: We men on both sides and the relationship between the two during the campaigns in the Mediterranean and northwest Europe are often cited as an example of harmonious cooperation.

As a correspondent in both theaters of war, I concur. But there were major differences between the situation then and today.

The first, and probably most important, was that total censorship prevailed. Everything written, photographed or broadcast was scrutinized by censors. Anything that did not meet the high command's considerations of security was deleted.

A second difference was that television did not exist as a news media during World War II. The "loss" of the Vietnam War is attributed by extremists in the American military to television's capacity to bring its horrors into American living rooms. What, then, would have been the reaction of the Allied publics had the bombing of London, the slaughter at Anzio or the house-to-house and room-to-room fighting at Stalingrad been brought into their homes?

The third factor was the attitude of the correspondents themselves. There was resistance to censorship during World War II but situations in which a reporter tried to evade it with material that might endanger soldiers' lives or ships at sea were extremely rare.

Censorship was intended to apply only to military matters. Concern over a spate of unfavorable reports on the political situation in North Africa following the assassination of Adm. Jean François Darlan prompted Gen. Dwight D. Eisenhower, Supreme Commander of Allied forces, to impose a political

censorship for a time. But a storm of protest from American and British politicians, as well as from the media, forced the high command to discontinue the practice.

The existence of military censorship did, however, enable commanders to talk with a freedom absent in later wars. World War II correspondents were permitted, if not encouraged, to interview officers dealing with operations, intelligence or military government. Corps, divisional and brigade commanders were accessible on the various fronts. General Eisenhower took the lead, providing full and detailed briefings before each major operation. Responsible reporters, he believed, helped sustain popular support for the war, and censorship took care of any inaccuracies that might creep into their stories.

Along the fronts in Tunisia, Sicily, Italy and northwest Europe, reporters had complete freedom of movement. If they risked their lives by moving too close to a fire fight or by flying on bombing missions over Berlin, that was their concern. In all, about 140 correspondents were killed on all fronts during World War II.

World War II was the last in which total censorship prevailed. The change in the media-military relationship began during the Korean War, when what censorship occurred was largely imposed at the source by senior officers. The main source was Gen. Douglas A. MacArthur, Commander of United Nations Military Forces in South Korea, a master at putting across the military's view of operations, and at keeping his mouth shut about impending campaigns.

Censorship at the source reached its apogee in the Vietnam War. On the whole, reporters were free to go where they wished, but those who did not have the trust of senior officers, a trust laboriously built in past wars, were given little information. Many officers became increasingly convinced that the growing hostility to the war on the part of the American public was due to biased and inaccurate reporting by correspondents.

(Continued on Page 61)

This situation was exacerbated by the widespread belief among military personnel that the news media, by emphasizing in print and pictures the enemy's foray into the United States Embassy in Saigon, had obscured the true dimensions of their victory in the Tet offensive in 1968.

That view was disavowed in a recent Columbia Journalism Review article by Charles Mohr of The New York Times, one of the most respected correspondents in Vietnam. He and other reporters, Mohr wrote, did not "give the embassy attack prolonged, obsessive coverage while ignoring the subsequent course of battle."

After Tet, reporters were often attacked by officers for giving false impressions. Flying in a helicopter with a colonel of infantry, I, for instance, was told that the valley below us had been completely pacified — we put down at one village to prove the point — but that "your damned newspaper and the damned TV make it sound like a hotbed of Vietcong guerrillas."

The armed forces emerged from the Vietnam War psychologically scarred. They were embittered by their failure to defeat the Vietnamese because of what they considered political manipulation in Washington and, above all, by the media's treatment.

The inability of the military in the field to comprehend the intricacies of television journalism was one reason enmity reached such proportions. The military did not realize that prime time, no matter how important the material, is short, and that the electronic media's news editors are likely to pick the most sensational shots.

These photographs may be gory. War is gory. But to argue, as some officers still do, that such selections were made to intentionally reduce popular support for the war is nonsense. So is the contention that this support was lost in American living rooms. The Vietnam War was lost, if indeed it was lost in the military sense, on university campuses and in the Congress.

The search for truth begins with a skeptical attitude. Most reporters, especially those who have dealt with

governments, develop this attitude early in their careers. It is seldom encountered in government public-relations people whose jobs and careers depend on accepting and relaying what they are told by those in higher echelons. Newly designated press officers receive instruction in how the media works at special courses conducted at Fort Benjamin Harrison in Indiana. Particular attention is paid to the media's problems of time and space, and how best to utilize that knowledge in presenting the military's position in the best possible light.

□

The military is not solely responsible for muzzling the press during the first days of the Grenada operation. Blame must also be attached to the Reagan Administration, which, though constitutionally in control of the military, abdicated that control when media accessibility came up for discussion before the operation began. It was James A. Baker 3d, then White House chief of staff, who accepted on behalf of the President restrictions imposed by the military on the media. He has since said he would do it again in a similar situation involving what he has called a "commando raid."

Danger to correspondents was cited by Baker and others as a reason for the exclusion. But reporters had gone on similar commando raids during World War II. They were also present during fierce fighting at Alamein, Tunis, Salerno, Anzio, Iwo Jima and Guadalcanal and a hundred other battlefields in Europe and the Pacific. Danger is part of a war correspondent's job. Every reporter, every editor knows that. But they also know that battles have to be covered, and that the media, not the military, is the best vehicle for conveying what occurred.

What about military security? If the Administration feared that some correspondents selected to accompany the invading forces would reveal the facts in advance, there were ways to prevent that. A pool of correspondents could be taken to a military compound where they would be informed of what was

(Continued on Page 83)

*"Barring reporters
from the battlefield"*

NYT Mag. Feb. 5, 84

about to happen and assured that when the time came they would go in with the first wave. There are precedents for such an action. Before the raid on Dieppe during World War II, for example, reporters were spirited away to Bath in England and kept incommunicado for four days before joining the units to which they had been assigned. This procedure was employed again recently by the British who, after keeping their press under wraps at sea, permitted reporters to go ashore with landing teams sent to regain the Falklands from the Argentines.

Another excuse put about by the American military for excluding the press in Grenada was that some new techniques were to be employed in the invasion. If they were, they were not evident to knowledgeable observers. Dropping Rangers and airborne troops from 500 instead of 300 feet is not a new technique but rather a tactical change enforced by the exigencies of combat.

A Navy source has suggested that the use of the service's Seals (sea, air and land underwater demolition and landing teams) was an innovation. Again, nonsense. Similar operations by Britain's Special Boat Squadron were employed and reported on in detail during the Falklands operations.

The impression left by the American Government's reporting of the first two days of the Grenada operation leaves the distinct feeling that the objective was not to present the full facts of the matter but rather to make the most favorable impression on the public at large.

What if the operation had

gone wrong? Would the Government have told the public that an ill-assorted group of Grenadians and Cubans was kicking the tripe out of some of our finest troops?

□

The continuing dispute over the restrictions placed on the media in Grenada reached a good deal further than that tiny Caribbean island. This is a period of limited, local wars — Grenada, Lebanon, the Falklands — any of which by a combination of circumstances can expand into a deadly serious conventional war in which vastly greater forces could quickly become involved.

Can the American people,

whose servants are both the military and any Administration, be fed pap churned out by the powers that be? Everything in our experience shows that even if they are they will soon discern the truth behind the headlines.

The present tendency to muzzle the media is dangerous. Democracies only win wars when they have popular support. That support can only come from an informed public. If there is censorship, then let it be flexible enough to tell the bad with the good. If correspondents are killed, so be it. A lot of good men will die. These are dangerous times. Only an informed America will weather them. ■

*Missing Reporter from the
Battlefield "*

NyT Mag Feb. 5, 84

WASHINGTON POST

A28

... R

Sunday, May 6, 1984

THE V

U.S. Bars Reporters From Naval Exercises

SAN SALVADOR, May 5 (UPI)—U.S. military officials say American journalists are not allowed to visit U.S. vessels participating in joint naval exercises in the Gulf of Fonseca.

It was believed to be the first time Pentagon officials had told journalists they could not observe American military war games in Central America.

"The American Navy is not embarking any newspapermen," said Col. Richard Lake, a Pentagon spokesman who yesterday turned down a request by United Press International and the The Washington Times to visit the exercises.

He gave no reason why the exercises, designed to improve the capacity of Honduras and El Salvador to stop arms traffic to Salvadoran guerrillas, were under a news blackout.

The U.S. Destroyer USS Deyo and the guided missile frigate USS Reid have been leading the joint exercises in which the Honduran and Salvadoran navies are participating.

The war games started April 26 and are scheduled to end May 7.

Pentagon Plans Media Pool to Cover Missions

By Fred Hill
Special to The Post

The Defense Department is preparing to designate a rotating pool of reporters who could be called at a moment's notice to cover military operations or other operations, according to Michael J. Burch, assistant secretary of defense for public affairs.

The media pool would be expected to operate in secrecy as an act to tip off other reporters until the operations begin, Burch said. The Pentagon would select physically fit reporters from organizations agreeing that "the security of our mission and the safety of our forces" are paramount, he added.

The formation of a media pool, which is still in the planning stages, grew out of the military's experience during the invasion of Grenada last October, when all reporters were excluded from the Caribbean island until the third day of battle. A number of news organizations complained that the Defense Department had used the pretext of security to keep them away from the fighting longer than necessary.

Burch said yesterday that Defense Secretary Casper W. Weinberger believes that the press was handled properly during the Grenada operations and that, given the same circumstances, Weinberger would exclude the press again. But Burch also said that, with the establishment of a media pool and other procedures, reporters could be allowed to witness possible future

Pentagon Plans Rotating Media Pool Able to Respond at Moment's Notice

crises" the pool, calling reporters without warning and taking them to report to Andrews Air Force Base for what turns out to be mock operations. That would show the Pentagon whether the system works and whether reporters could be treated with secret information, and it would mean that reporters could not assume from a call-up that a real war was about to start.

Formation of a pool for emergencies is mentioned in a report on military relations released by the Pentagon yesterday. The report, written by a panel of active and retired military public information officers and retired journalists, did not recommend such a pool but said the defense secretary should study the idea.

The panel, chaired by retired Army Maj. Gen. William Soble, did make several recommendations that Weinberger endorsed and that Burch said have been implemented or soon will be. Many of them focus on encouraging military commanders to remember the needs of the press early in the planning process.

"There was not sufficient public affairs awareness on the part of commanders and planning staff," Burch said. "At times, public affairs was not brought in very early in the process."

As a result, exercises and contingency manuals have been rewritten and a "public affairs cell" within the Joint Chiefs of Staff has been provided for, Burch said that he has met with top military commanders

around the world, urging them to consider the facilities reporters would need for transportation and filing stories and to add a public affairs component to their regular war games.

"No commander is ever going to want you to take the seat of a soldier or to take the space of a host of amenities," he said. But he said that better planning could get the press "prepositioned" and into the battle more quickly.

The Pentagon also is establishing "general ground rules for combat coverage," Burch said. He said there is no discussion of imposing curfew, but that anyone who violated the ground rules would be removed and not permitted to cover future operations.

Weinberger also announced that he will form a Media Advisory Committee of "ambient journalists and former war correspondents to advise me" on the best ways to allow maximum news media coverage of military operations consistent with security.

Burch would not disclose the names of those serving on the committee, but sources said it was essentially the same group that Weinberger assembled and consulted secretly last spring. That group included authors Theodore H. White and James A. Michener, CBS newscaster Walter Cronkite and Eric Sevareid, Boston Globe reporter William Beecher, NBC reporter Jack Reynolds and photographer Edward T. (Eddie) Adams.

Pentagon Forms War Press Pool; Newspaper Reporters Excluded

By RICHARD HALLORAN

Special to The New York Times

WASHINGTON, Oct. 10 — Defense Department officials today disclosed the makeup of a press pool the Government would form to cover the initial stages of any surprise military operations. It would include news agency, radio, television and magazine reporters but not reporters from individual newspapers.

The news agencies to be included in the pool, Associated Press and United Press International, send their reports to newspapers as well as to television and radio stations. Representatives of many newspapers protested exclusion of their reporters and said they would call for revision of the pool planned by the Defense officials.

Defense officials said the organizations to be represented in the pool, which was set up in answer to criticisms from the press over limits on coverage of the invasion of Grenada last year, had been picked by the Defense Department but that the news organizations could choose the correspondents. They said the pool should be ready to cover military contingencies on short notice.

The officials said the Defense Department had proposed ground rules, similar to those used during the war in Vietnam, to govern the coverage. Those proposals are being studied by the organizations that have been selected and are not yet final, the officials said.

The pool would include two news agency reporters, one radio correspondent, four television reporters plus a camera operator and a sound technician, a still photographer and a magazine writer, for a total of 11 men.

The Pentagon pool would be unusual in at least two respects:

Its composition would be determined solely by the Government. Traditionally, Government agencies have established the need for a pool when coverage had to be reported because of limited space or treatment, but worked out composition of the pool in cooperation with members of the press.

Newspapers have been left out. In most press pools in the past, representatives of all segments of news communications have been included, with priority given to news agencies when space was severely limited.

The Pentagon officials said reporters from newspapers had been excluded because they thought the newspapers' needs could be filled by news agencies.

They also said the large number of newspapers made negotiating with them difficult.

Moreover, some officials said privately, senior Pentagon officials had expected more resistance to proposed ground rules for coverage from newspapers than from other news organizations because newspapers have usually taken more independent stands against restrictions.

The issue of coverage of military operations erupted a year ago when President Reagan ordered the Grenada invasion. At the request of the Joint Chiefs of Staff, Secretary of Defense Casper W. Weinberger prohibited coverage of the initial stages of the operation and permitted only limited reporting until it was nearly over.

That provoked a wave of protests from most news organizations, although polls indicated a majority of the public initially supported the exclusion. News executives cited the Grenada restrictions as a departure from a long history of war correspondence dating from the Civil War.

In response to the protests from news organizations, the Chairman of the Joint Chiefs of Staff, Gen. John W. Vessey Jr., formed a panel of officers and journalists led by a retired Army public affairs officer, Maj. Gen. Winant Sibley, to take testimony from news executives.

Several Executives Astonished

Today several newspaper executives reacted with astonishment to the Pentagon's announcement of the pool and said they would seek revision of the decision.

Arthur Ochs Sulzberger, publisher of The New York Times, said in a statement: "The Defense Department's plan to ban newspaper reporters from selected military operations is incredible. It reveals the Administration to be out of touch with journalism, reality and the First Amendment. "From the earliest days of this republic, newspaper reporters have had a long and honorable relationship with our nation's soldiers. If any coverage anywhere does ever have to be limited, it is impermissible that Defense Secretary Weinberger should be the one to choose his favorites.

"The New York Times's duty to its readers will find us making strenuous

efforts to reverse this whole approach and this blatant act of discrimination."

The chairman of the American Newspaper Publishers Association, Richard J. V. Johnson, president of The Economist Chronicle, said in a statement: "We are pleased that the Department of Defense has taken the first step toward creating an effective contingency press pool for U.S. military operations. Obviously, a pool of 11 must include at least one experienced daily newspaper reporter and we have asked the Pentagon to make that correction promptly."

Seymour Topping, managing editor of The New York Times, said The Times intended to join other newspaper organizations in protesting the decision. "The special needs of newspapers in serving their readers cannot be fully met by news agency reports," he said.

Albert R. Hunt, Washington bureau chief of The Wall Street Journal, called the decision "outrageous and unacceptable," saying "the notion of not having a single newspaper in a pool is unprecedented." He added: "I have never heard of a pool arrangement that totally excludes newspapers. It would appear that they are not anxious to give any or possibly in-depth reporting on this."

Benjamin Bradlee, executive editor of The Washington Post, said, "The Washington Post will do everything it can to report the news on what we are in any pool or not."

'Standard Degree Possible'

Reached in Gettysburg, Tenn., where directors of the American Association of Newspaper Editors opened a board meeting today, Richard D. Snyder, the association president, said: "I can't speak for the board, but my personal opinion is that there is a great void there. I am certainly disturbed that there is no provision for daily newspapers. Our freedom of information committee is here. It is fortunate that we are all meeting here to consider this."

In its report in August, the Pentagon panel said: "It is essential that the U.S. news media cover U.S. military operations to the maximum degree possible, consistent with national security and the safety of U.S. forces."

But the Pentagon's chief spokesman, Michael I. Burch, made clear in a briefing on that report that the Secretary of Defense "can dictate a national policy on how an operation is covered." A news pool, Mr. Burch said, "will more or less be selected by us." He added, "There will be some consultation, but the final decision is ours."

The Pentagon officials said Mr. Burch met a week ago with the chiefs of television, radio, magazines and news agency bureaus here to lay out his decision and to propose a set of ground rules intended to provide security for military forces.

APPENDIX II-BB

Letters

The Committee on the Judiciary received a number of letters concerning the hearings entitled "1984: Civil Liberties and the National Security State." The following is a selection of letters, reprinted with permission.

November 4, 1983

U.S. House of Representatives
Judiciary Committee
Washington, D.C

Gentlemen:

I recently observed David Brinkley, John Chancellor and others appear before your Committee to present their case against President Reagan's decision not to have the TV and press with the Grenada invading troops.

The reasons they gave appear very shallow and self-seeking to me. The idea that every important event must be accompanied by TV cameras is stupid. We Americans are tired of TV telling us what we should be doing and how we should feel about the important events in our lives. In my opinion the TV people should stick to reporting the news, not managing it as they now seem to try to do.

As a parent of a student attending St. Georges University School of Medicine, I wholeheartedly support the action of our President. His decision not to allow the TV along, in my opinion, was wise and just. The American people are not crying out that they were deprived of TV coverage, only the networks and their eternal battle for Nielson ratings and thus ability to charge advertisers more and more money seem to care.

The American public is contantly bombarded every evening from 5 P.M. to the wee hours of the morning with TV news. Not to mention early in the morning until about 8:30 A.M. We could do with a lot less coverage.

Respectfully,

Thomas J. Roche, Jr.
7 Summit Rd.
Brookside, N.J. 07926

Montgomery Hollow
Roxbury, N.Y. 12474
October 30, 1983

The Hon. Robert W. Kastenmeier
House of Representatives
Congress of the United States
Washington, D.C. 20515

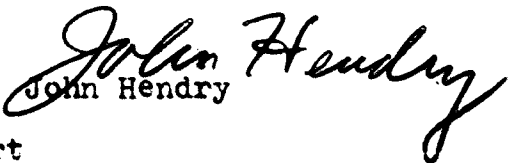
Dear Rep. Kastenmeier:

I was very encouraged and relieved to learn that the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice will soon begin hearings on the relationships between civil liberties and the so-called "national security state."

The current Administration's passion for secrecy in government -- demonstrated in its new dragnet lie-detector policy, its government-employee censorship order, and most recently its control of press coverage of the Grenada invasion -- makes these hearings terribly important.

I fear the growth of governmental secrecy more than I do any other national or international threat including thermonuclear war. Neither the Soviet nor the American government wants atomic war -- but both very much want more government secrecy; and this is very, very frightening.

Yours truly,


John Hendry

CC: The Hon. Sherwood Boehlert
The Hon. Jack Brooks
The Hon. Daniel Patrick Moynihan
The Hon. Alphonse D'Amato

305 Maxwell Lane
Newport News, VA 23606
November 8, 1983

Hon. Robert W. Kastenmeier
Chairman, House Judiciary Subcommittee on
Courts, Civil Liberties and the
Administration of Justice
Reyburn Bldg., Room 2137
Washington, D.C. 20515

Dear Sir,

I have read accounts of the hearings being held by your subcommittee into the conflict between the need for information and national security. In particular, I have noticed that testimony being reported in the newspaper articles has been by the news media and professionals.

I am enclosing for your information, a copy of my letter to National Broadcasting Company dated October 27, 1983 following the rescue mission on Granada and following Mr. Chancellor's commentary on the NBC Evening News on October 26, 1983. I believe the feelings expressed in my letter represent those of a great number of the private citizens in the United States of America concerning the attitude and lack of responsible behavior by the news media in general and the TV Networks in particular.

I trust that your hearings will be thorough and representative of the best interests of this country as a whole rather than that of any special business or political pressure group.

Very truly yours,

Ralph D. Bradway

Ralph D. Bradway

RDB/jb

305 Maxwell Lane
Newport News, VA 23606
October 27, 1983

Mr. Grant Tinker, Chairman and C.E.O.
National Broadcasting Company
30 Rockefeller Plaza
New York, N.Y. 10019

Dear Sir:

After watching your NBC News at 6:30 PM Wednesday, October 26, 1983, I find myself compelled to express to you as head of NBC my deepest feelings of dismay at the low levels of professionalism your news programming has achieved.

Mr. Chancellor's commentary was a disgrace to you and to all honest journalism. His vitriolic attack and tirade against the President of the United States and the U.S. Government was not only uncalled for but entirely out of order. The hate that prompted his commentary was evident in his eyes and his posture during his presentation.

Apparently Mr. Chancellor believes that he and others of the news media are over and above everyone else and should be subject to no control whatsoever and can attack anything or anybody with which they disagree.

I deplore that the philosophy of anticipating, shaping and controlling news has replaced the reporting of news as the standard for American journalism.

It would be refreshing to see a return to a higher standard of conduct. Until then, I and others with whom I have discussed this will no longer be watching NBC News.

Very truly yours,



Ralph D. Bradway

cc: Mr. Robert Mulholland, President
Mr. Reuben Frank, NBC News

Elbert N. Mullis, Jr.
POST OFFICE BOX 2006
BIRMINGHAM, ALABAMA 35201

November 4, 1983

Congressman Robert W. Kastenmeier
United States House of Representatives
2232 Rayburn Building
Washington, D. C. 20515

Dear Congressman Kastenmeier:

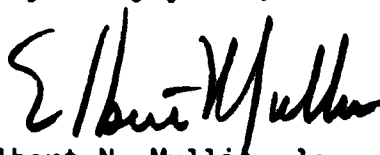
I am in full and complete support of our recent Grenada action and agree 100% with the decision to keep the news media out.

John Chancellor, David Brinkley and Edward Joyce are a bunch of cry babies because they were not informed of the advance planning and the action missed the morning news.

I see absolutely nothing of censorship or anything else of an unprecedented nature in this decision.

I want my letter placed before the House Judiciary Subcommittee on courts, civil liberties and the administration of justice as an American citizen who supports the President on his Grenada decision.

Very truly yours,

A handwritten signature in black ink, appearing to read "Elbert N. Mullis, Jr.", written in a cursive style.

Elbert N. Mullis, Jr.

ENM, JR:v

BYCO, INC.COMMERCIAL DEVELOPMENT - 3800 W. Coast Highway, Newport Beach, CA 92653 (714) 645-2251

November 4, 1983

MR. DAVID BRINKLEY
ABC TELEVISION
New York City, New York

Dear Mr. Brinkley:

I keep reading articles in the newspaper about the great "tragedy" that has struck our country as a result of you media folks being "denied" access to the Grenada action.

Your tears and moans have reached us all. The very dramatic presentation before the House Judiciary Subcommittee was "magnificent". I also weep for the media in all its forms - the only thing is that my tears are of joy, not of sadness. You fellows are long overdue for some wrist-slapping as a result of your misleading, distorted, biased, and, sometimes downright dishonest reporting of the news. I think our government is fully within its rights to keep the press from "screwing up" some of their more sensitive activities. You all get your crack at it sooner or later and we're not talking about total and forever isolation from the news.

When the media in total gets their act together and stops trying to create the news instead of report the news, you'll have more sympathy from this writer.

Sincerely yours,



S. H. Byers, President
BYCO, INC.

cc: Ronald Reagan, White House
House Judiciary Subcommittee on Censorship. ✓

■ HOW I GOT THE N.S.A. FILES. . .

How Reagan Tried To Get Them Back

JAMES BAMFORD

On September 22, 1981, the Federal government did something it had never done before. The Justice Department, for the first time in its history, issued an order forbidding an author from publishing previously released official documents in his possession and demanding their return. The documents, said the department, had been "reclassified."

Three years earlier I had begun work on *The Puzzle Palace*, the first book-length study of the National Security Agency. As part of my research I had submitted a Freedom of Information Act request to the Justice Department for documents relating to its highly secret investigation into the illegal use of electronic surveillance by the N.S.A. and the Central Intelligence Agency. The investigation had its roots in a 1974 article by Seymour Hersh in *The New York Times* that revealed details about a massive domestic intelligence operation, code-named Operation Chaos, run by the C.I.A. In response to the article, President Ford in January 1975 named Vice President Rockefeller to head a commission to look into C.I.A. activities in the United States.

The Rockefeller Commission's final report, issued on June 6, 1975, noted that the intelligence community had engaged in a number of questionable electronic surveillance activities. As a result of the report, Attorney General Edward H. Levi established a secret internal task force to determine the full extent of governmental electronic surveillance in the country.

Over the next year, the task force probed more deeply into the problems of domestic eavesdropping than any part of the executive branch had ever done before, and on June 30, 1976, it issued its final report. Classified "TOP SECRET UMBRA/HANDLE VIA COMINT CHANNELS ONLY," the 175-page document detailed twenty-three categories of questionable eavesdropping operations. Although some activities were immune from prosecution because of the statute of limitations, others were not. "This electronic surveillance activity," said the report about one N.S.A. program, Operation Minaret, "presents prima facie questions of criminality and is well within the limitations period."

Nevertheless, because there appeared little likelihood that convictions could be obtained on the basis of the evidence, and because of the possibility that the defense would resort to "graymail," the report recommended that the inquiry be terminated for "lack of prosecutive potential."

James Bamford holds a Juris Doctor degree and is the author of the recently published The Puzzle Palace: A Report on NSA, America's Most Secret Agency (Houghton Mifflin).

The information was considered so sensitive that only two copies of the task force's report were produced. One of these was given to George W. Calhoun, chief of the Justice Department's special litigation unit. His job was to examine the legal issues and determine whether or not to prosecute. In his "Prosecutive Summary," issued on March 4, 1977, he recommended to Robert L. Keuch, Deputy Assistant Attorney General in the criminal division, that the investigation be terminated.

A year and a half later I submitted my F.O.I.A. request. When it arrived at the Justice Department, it was sent to Keuch, who determined that it would apply to the final report of the task force as well as to Calhoun's "Prosecutive Summary." Because of the sensitivity of the documents, Keuch assigned Calhoun to review the materials already in the public domain and to base his declassification decision on that survey. He also decided not to submit the documents to the N.S.A. or the C.I.A. because the agencies were the principal subjects of the investigation and he felt that allowing them to review the reports would subvert the criminal justice system.

After ten months, on July 5, 1979, Keuch released the requested documents to me, with some portions deleted.

Several months later the N.S.A. became aware of Keuch's actions and requested that the Justice Department send it copies of the same documents. After a review, N.S.A. Director Adm. Bobby R. Inman wrote to Attorney General Benjamin Civiletti, informing him that the documents contained still-top-secret information and that they should never have been released without first being sent to the N.S.A. Civiletti, believing that the documents had been properly declassified or else realizing that the executive order on classification forbade reclassifying documents released under the F.O.I.A., ignored Inman's protest.

On March 23, 1981, while working on the chapter of my book dealing with the close relationship between the N.S.A. and its supersecret British partner, Government Communications Headquarters in Cheltenham, I sent a letter to George M. (Bill) Gapp, the British senior liaison officer at the N.S.A. In the letter I noted that documents released to me by the government implicated his organization in Operation Minaret, the illegal N.S.A. program directed against American citizens. I asked whether he knew of his organization's involvement in the operation and whether it was currently engaged in any similar activities in the United States. Three weeks later a letter was hand-delivered to my Washington office by the British Embassy, informing me that "it is not the policy of Her Majesty's Government to answer enquiries of this nature."

Apparently notified of my letter by Gapp, N.S.A. Director Lieut. Gen. Lincoln D. Fawcett, Inman's replacement, sent a letter to Attorney General William French Smith, requesting another copy of the two Justice Department documents. Smith sent copies to both the N.S.A. and the C.I.A. The two intelligence agencies then identified for the Justice Department a total of 161 lines and another seventy-seven words on thirty-four pages covering fourteen spe-

pieces of information that should be reclassified "TOP SECRET UMBRA."

On July 8, 1981, just over two years after the documents had been released to me, I received a telephone call from Gerald A. Schroeder, a senior attorney with the Justice Department's secretive Office of Intelligence Policy and Review. He asked whether we could discuss a matter concerning the two documents released to me in 1979. I agreed, and on July 23, we met in the conference room of the Center for National Security Studies in Washington. Also present was my attorney, Mark H. Lynch, a senior staff attorney with the American Civil Liberties Union and one of Washington's leading authorities on national security law.

During the hour-and-a-half meeting, Schroeder said that the two documents had been released "by mistake," that the N.S.A. and the C.I.A. had determined they contained still-classified information and that the Justice Department would like me to return them for further deletions.

I informed Schroeder that I had had the material for two years, that it was already incorporated into my manuscript, that the Carter Administration had believed the information should be declassified and that in any case Executive Order 12065 stated that "classification may not be restored to documents already declassified or released to the public" under the F.O.I.A. In addition, I said that because the information related to illegal activities on the part of the N.S.A. and the C.I.A., I felt it was important for the American public to be informed. Under the circumstances, I told him, I would consider returning the material only if the

N.S.A. released to me other agreed-on information relating to the various illegal operations or allowed me to interview a knowledgeable official on the subject. Schroeder said he would have to check my proposal with N.S.A. and C.I.A. officials and would let me know.

The proposal was not unprecedented. About a year and a half earlier I had negotiated a similar agreement, with N.S.A. general counsel David C. Schwartz. Although under Public Law 86-36 the N.S.A. is virtually excluded from the Freedom of Information Act, I had discovered a loophole in the law that enabled me to obtain more than 6,000 pages of internal N.S.A. newsletters. Of concern to the agency, however, was the fact that scattered through these newsletters were the names and faces of a large percentage of its work force. Appreciating the N.S.A.'s problem, and having no real need for the name of every employee, I agreed not to contest the deletion of the names and photographs, providing Schwartz prepared for me a document detailing the N.S.A.'s entire organizational structure, including the names, titles and internal codes of the senior staff between 1975 and 1980. The proposal was agreed to and in February 1980 I was handed a document that listed more than forty officials.

Following approval—from Director of Central Intelligence William J. Casey, C.I.A. Deputy Director Bobby Inman and N.S.A. Director Fawcett—Schroeder informed me that he could arrange a meeting to discuss my proposal. We agreed to meet on August 14 in the editorial conference room of my publisher, Houghton Mifflin, in Boston.

Schroeder was accompanied by general counsel Schwartz and Eugene F. Yates, the N.S.A.'s Director of Policy. Shortly after the meeting began Schroeder, apparently under pressure from the N.S.A., sought to expand the scope of the meeting by bringing up the question of who else had seen or had copied the documents. This greatly complicated matters. Because the original purpose of the meeting was simply to discuss a compromise proposal, my attorney, as Schroeder knew, had decided not to attend. I asked Schroeder to telephone Lynch from the conference room and explain that he wanted to broad the agenda.

At one point during their telephone conversation, Schroeder brought up the possibility of using the espionage statute to force the return of the documents. Upon hearing this, Lynch asked to speak with me privately. Once the three officials had left the room, Lynch expressed worry over the tone of the meeting and the fact that I was alone and unrepresented. He advised me to put down the receiver, call Schroeder to the phone, then turn toward the door and keep walking. I agreed, and still have no idea when or how the three officials found their way out of Houghton Mifflin.

Despite the walkout, Schroeder was still interested in negotiating a settlement, but it now appeared that a reasonable solution would be impossible. There was some information, such as the N.S.A.-British link, that I would never compromise on, and I felt certain that the N.S.A. would also view the same information as non-negotiable. I therefore informed Schroeder that I was going to use the documents fully in my book and that all further discussions would be pointless.

On September 24, 1981, I received a registered letter stating: "You are currently in possession of classified information that requires protection against unauthorized disclosure. . . . Under the circumstances, I have no choice but to demand that you return the two documents. . . . Of course, you will have a continuing obligation not to publish or communicate the information."

As if to underscore the point, the Justice Department sent my attorney a letter on November 27 stating that "there should be no misunderstanding of the Government's position that Mr. Bamford holds information that is currently and properly classified" and that failure to return the documents could force the department to resort to an unnamed "post-publication judicial remedy."

Despite the threats, I refused to alter my manuscript or return the documents. From the very start of my research I was aware of the potential for serious problems over my choice of topic. There was probably no cow more sacred within the Federal government than the N.S.A., and no subject more sensitive than signals intelligence.

In 1931 Herbert O. Yardley wrote his classic book, *The American Black Chamber*, which set off such a national security storm that his widow, Edna, waited half a century before granting permission for a paperback edition—and then only after requesting and receiving permission from the N.S.A. In 1932 Yardley turned out another manuscript about the Black Chamber, this one ghost-written by Marie Stuart Klooz, a young freelance. Titled *Japanese Diplomatic*

Secrets, 1921-1922, it became the first and only manuscript in U.S. history to be seized and impounded by the Federal government for national security reasons. It was not until 1979 that it was, at my request, fully declassified.

Finally there was David Kahn, author of *The Codebreakers*, the monumental study of the history of cryptology which included a chapter on the N.S.A. The agency considered everything from physical surveillance to a black-bag job at Kahn's Long Island home to obtain his manuscript. "Disparaging" reviews were drafted and his name was placed on the N.S.A. "watch list," thus subjecting his communications to the N.S.A.'s sophisticated eavesdropping techniques. The agency eventually convinced Kahn's publisher, Macmillan, to secretly give it a copy of the manuscript for review. After first demanding the elimination of the entire chapter on the N.S.A., the agency settled for a single page. A copy of that page was obtained from the papers of a former senior N.S.A. official, and is included in my book.

In light of the foregoing, I was hardly surprised by the letter from the Justice Department. What was surprising, however, was the theory of reclassification. Seldom has the involvement of politics in secrecy been illuminated more clearly. Under the Carter Administration, the Justice Department decided to release the two documents. There was no "mistake." Even Gerald Schroeder has acknowledged that Keuch had for many years been the most experienced official in intelligence and national security matters at the Justice Department; Calhoun had spent ten months studying what could properly be released from the two documents. Both concurred on the declassification. And Civiletti personally went over the summary—and, most likely, the task force report—yet as Attorney General he chose to ignore the N.S.A.'s call for secrecy. That they could have let slip any part of these documents "by mistake" seems utterly inconceivable.

It is one thing for an Administration to adopt a stricter standard of secrecy than its predecessor's. It is entirely another thing to try to enforce that standard retroactively on people who had obtained declassified materials under preceding Administrations. Yet that is precisely what the Reagan Administration attempted to do in my case. The problem was Executive Order 12065, which prohibited such actions. To overcome this, President Reagan on April 2 issued a new executive order on secrecy which permits the President or an agency head to "reclassify information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security, and (2) the information may reasonably be recovered." When questioned by the press as to the meaning of the term "reasonably," the Administration refused to rule out the use of surreptitious entry. The new executive order took effect on August 1.

About 350 years ago, Cardinal de Richelieu, chief minister to King Louis XIII, declared, "Secrecy is the first essential in affairs of the State." With his new executive order on secrecy, President Reagan has said the same thing. □



Office of the Attorney General
Washington, D. C. 20530

March 11, 1983

MEMORANDUM

TO: Heads of Offices, Boards,
Divisions and Bureaus

FROM: William French Smith *WFS*
Attorney General

SUBJECT: Presidential Directive on Safeguarding
National Security Information

The President has issued a directive to strengthen our efforts to safeguard national security information from unlawful disclosure. This directive, a copy of which is attached, is based upon the recommendations of an interdepartmental group chaired by the Department of Justice. I fully support the President's policy and expect that it will be faithfully implemented throughout the Department.

This directive does not alter the existing obligation of Department personnel to comply with statutes and regulations pertaining to national security information. We must be careful to avoid the unnecessary or improper use of classification. Whenever possible, information should be kept unclassified or declassified so as to permit public access. However, information that is properly classified in the interest of national security must be protected from unauthorized disclosure.

Many of the specific requirements of the directive involve no change from current Department of Justice policy.

- The use of nondisclosure agreements and the requirement of prepublication review in appropriate cases are consistent with current policies. More detailed guidance on these policies will be provided in the near future.
- The directive requires no change in existing Department policies on use of the polygraph, with regard to attorneys or FBI employees. Policies with regard to employees in the competitive service will be changed to conform with expected revisions in OPM regulations on this subject.
- Internal investigations of unauthorized disclosures will continue to be coordinated by the Office of Professional Responsibility, with assistance from the FBI as needed.

To the extent implementation of the President's directive requires changes in Department of Justice policies and procedures, you will be kept fully informed.

Embargoed for Conclusion of Background Briefing
Held March 11, 1983, at the Department of Justice

Fact Sheet

Presidential Directive on
Safeguarding National Security Information

Background

- Unlawful disclosures of classified information damage national security by providing valuable information to our adversaries, by hampering the ability of our intelligence agencies to function effectively, and by impairing the conduct of American foreign policy.
- The President has issued a directive requiring that additional steps be taken to protect against unlawful disclosures of classified information.
- This directive is based on the recommendations of an inter-departmental group convened by the Attorney General.

Scope of Directive

- The directive deals only with disclosures of classified information.
- By Executive Order, the only information that can be classified is information which "reasonably could be expected to cause damage to the national security" if released without proper authorization. (E.O. 12356 § 1.1(a)(3).)
- The Executive Order also prohibits the use of classification to conceal violations of law, inefficiency or administrative error, or to prevent an embarrassment to a government agency or employee. (E.O. 12356 § 1.6(a).)

Summary of Provisions

- The directive imposes additional restrictions upon government employees who are entrusted with access to classified information, and upon government agencies that originate or handle classified information.
 - More employees will be required to sign nondisclosure agreements, including provisions for prepublication review, such as were approved by the Supreme Court in United States v. Snepp (1980).

Agencies will be required to adopt policies concerning contacts between journalists and persons with access to classified information, so as to reduce opportunities for unlawful disclosures. However, no particular policies are mandated in the directive.

- Agencies will be required to adopt new procedures so that unlawful disclosures of classified information will be reported and analyzed more efficiently.
- The directive establishes a new approach to investigating unlawful disclosures to replace the past practice of treating such matters as purely criminal investigations.
 - Although unauthorized disclosures of classified information potentially violate a number of criminal statutes, there has never been a successful prosecution. There are a number of practical barriers to successful criminal prosecution in most of these cases.
 - This directive clarifies FBI's authority to investigate unlawful disclosures of classified information, even though it is anticipated that a successful investigation will lead to administrative sanctions (such as demotion or dismissal) rather than criminal prosecution.
 - All agencies with employees having access to classified information will be required to assure that their policies permit use of polygraph examinations under carefully defined circumstances. The polygraph is already used on a regular basis by our largest intelligence agencies. The directive provides for a greater degree of consistency in government-wide policy regarding use of this investigative technique.
 - The use of the polygraph in any particular case will be subject to the discretion of an employee's agency head.
 - There will be no change in the current practice of targeting investigations at employees who are suspected of unlawfully disclosing classified information, rather than at journalists who publish it.

- The directive provides that employees found by their agency head to have knowingly disclosed classified information without authorization or to have refused cooperation with investigations will be subject to mandatory administrative sanctions to include, as a minimum, denial of further access to classified information. Existing procedural safeguards for personnel actions involving federal employees remain unchanged.

Expected Results

- This directive is not expected to eliminate all unlawful disclosures of classified information.
- The directive is designed to improve the effectiveness of our present program and, over time, to reduce the frequency and seriousness of unlawful disclosures of classified information.
- The directive also emphasizes that government employees who are entrusted with classified information have a fiduciary duty to safeguard that information from unauthorized disclosure.

Safeguarding National Security Information

As stated in Executive Order 12356, only that information whose disclosure would harm the national security interests of the United States may be classified. Every effort should be made to declassify information that no longer requires protection in the interest of national security.

At the same time, however, safeguarding against unlawful disclosures of properly classified information is a matter of grave concern and high priority for this Administration. In addition to the requirements set forth in Executive Order 12356, and based on the recommendations contained in the interdepartmental report forwarded by the Attorney General, I direct the following:

1. Each agency of the Executive Branch that originates or handles classified information shall adopt internal procedures to safeguard against unlawful disclosures of classified information. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. This requirement may be implemented prospectively by agencies for which the administrative burden of compliance would otherwise be excessive.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and other classified information. All such agreements must include a provision for prepublication review to assure deletion of SCI and other classified information.

c. All agreements required in paragraphs 1.a. and 1.b. must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States. The Director, Information Security Oversight Office (ISOO), shall develop standardized forms that satisfy these requirements.

d. Appropriate policies shall be adopted to govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures of classified information. All persons with authorized access to classified information shall be clearly apprised of the agency's policies in this regard.

2. Each agency of the Executive branch that originates or handles classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

e. Persons determined by the agency to have knowingly made such disclosures or to have refused cooperation with investigations of such unauthorized disclosures will be denied further access to classified information and subjected to other administrative sanctions as appropriate.

3. Unauthorized disclosures of classified information shall be reported to the Department of Justice and the Information Security Oversight Office, as required by statute and Executive orders. The Department of Justice shall continue to review reported unauthorized disclosures of classified information to determine whether FBI investigation is warranted. Interested departments and agencies shall be consulted in developing criteria for evaluating such matters and in determining which cases should receive investigative priority. The FBI is authorized to investigate such matters as constitute potential violations of federal criminal law, even though administrative sanctions may be sought instead of criminal prosecution.

4. Nothing in this directive is intended to modify or preclude interagency agreements between FBI and other criminal investigative agencies regarding their responsibility for conducting investigations within their own agencies or departments.

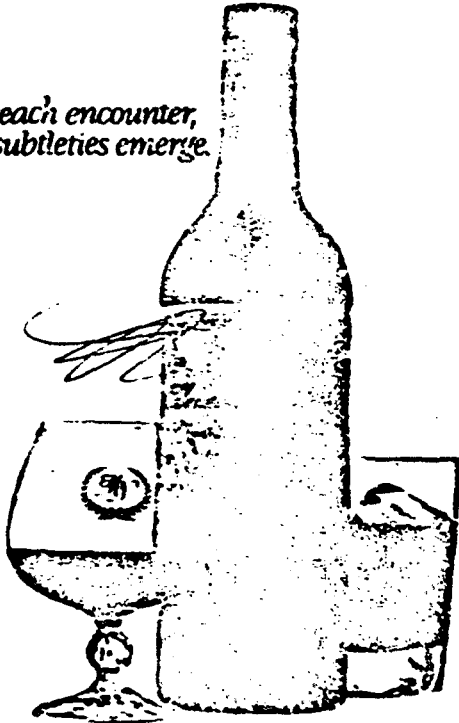
5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies, as necessary, so that employees may be required to submit to polygraph examinations, when appropriate, in the course of investigations of unauthorized disclosures of classified information. As a minimum, such regulations shall permit an agency to decide that appropriate

adverse consequences will follow an employee's refusal to cooperate with a polygraph examination that is limited in scope to the circumstances of the unauthorized disclosure under investigation. Agency regulations may provide that only the head of the agency, or his delegate, is empowered to order an employee to submit to a polygraph examination. Results of polygraph examinations should not be relied upon to the exclusion of other information obtained during investigations.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations, and guidelines.



*With each encounter,
more subtleties emerge.*

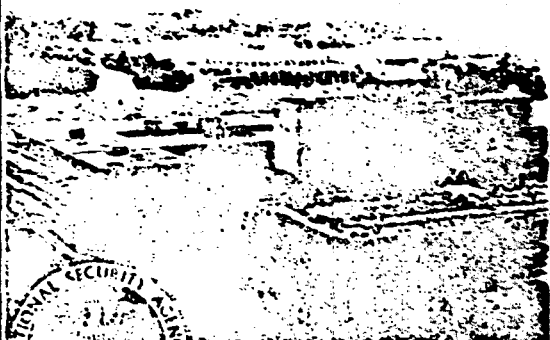


MANDARINE NAPOLEON
GRANDE LIQUEUR IMPERIALE

8102-64,46-46

U.B.25003.8 MAR 27 1973 FILE 671

THE SILENT POWER OF THE N.S.A.



From its headquarters in Fort Meade, Md., the National Security Agency directs electronic surveillance of the world's communications network. Recently, its reach has extended to private research in the area of

violated his Fourth Amendment right to be free of "unreasonable searches and seizures." Even while refusing the plaintiff's request for reconsideration, the Court curiously acknowledged the far-reaching nature of the case, recognizing that the N.S.A.'s interception of overseas telecommunications and their dissemination to "other Federal agencies has great potential for abuse." The Court, however, held that the problem was "a policy matter that lies in the domain of the executive or legislative branch of our Government."

By David Barabara

A Federal Court of Appeals recently ruled that the largest and most secretive intelligence agency of the United States, the National Security Agency, may lawfully intercept the overseas communications of Americans even if it has no reason to believe they are engaged in illegal activities. The ruling, which also allows government to use conversations to be sent to the Federal Bureau of Investigation, significantly broadens the already immense authority of the N.S.A. to keep track of American citizens.

The decision by the United States Court of Appeals for the Sixth Circuit involves the Government surveillance of Abdou Jabara, a Michigan-born lawyer who for over a year has represented Arab-American citizens and alien residents, and received a 1970 ruling that the N.S.A.'s acquisition of Jabara's overseas messages

The N.S.A.'s reach more than a massive crop of secret bases that collect, analyze and store information for the President and such dignitaries as the Central Intelligence Agency and F.B.I. The National Security Agency, an arm of the Defense Department but under the direct command of the Director of Central Intelligence, is an electronic spying operation, and its leverage is based on a massive bank of what are believed to be the largest and most advanced computers now available to any government in the world: computers to track codes, direct spy satellites, intercept electronic messages, surveil

David Barabara is a reporter in The Times's Washington bureau. This article is adapted from Mr. Barabara's book "The Rise of the Computer State," to be published by Doubleday, Garden City, N.Y.

New York Times Magazine
Mar 27, 1973

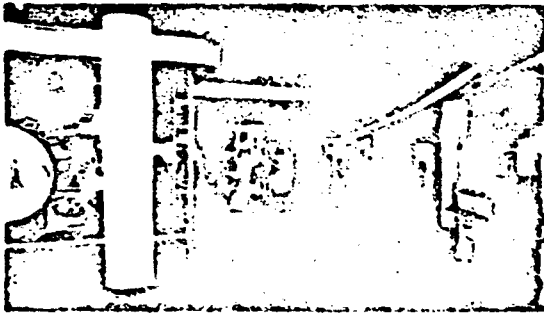
A WHITER SHADE OF PALE

Join the club at
Abraham & Straus,
G. Fox, Harz & Co.
and Wanamaker's.

SPORTO A.C.

SPORTO is a registered trademark of The Coldwell Banker Co., Boston, MA 02101.

The most important designer name in retail in 1983 is not Calvin Klein, Perry Ellis, Giorgio Armani or Sonia Rykiel. It's Mitchell Giurgola.



Call Dick MacNamara at (617) 227-6661 for more information. Structured for new use in the heart of downtown Boston.

Lafayette Place  **Structured For Success.**

also target words to spin communications and other, organize and index all of it.

Over the years, this virtually unknown Federal agency has repeatedly sought to enlarge its power without consulting the civilian officials who theoretically direct the Government, while it also has sought to influence the operation and development of all civilian communications networks. Indeed, under Vice Adm. Bobby Ray James, N.S.A. director from 1977 to 1981, the agency received an enlarged Presidential mandate to involve itself in communications issues, and successfully persuaded private corporations and institutions to cooperate with it.

Yet over the three decades since the N.S.A. was created by a classified executive order signed by President Truman in 1952, neither the Congress nor any President has publicly shown much interest in grappling with the far-reaching legal conflicts surrounding the operation of this extraordinarily powerful and clandestine agency. A Senate committee on intelligence, warning that the N.S.A.'s capabilities impinged on crucial issues of privacy, once urged that Congress or the courts develop a legislative or judicial framework to control the agency's activities. In a nation whose Constitution demands an open Government operating according to precise rules of fairness, the N.S.A. remains an unexamined entity. With the increasing "computerization of society, the conflicts it presents become more important.

The power of the N.S.A., whose annual budget and staff are believed to exceed those of either the F.B.I. or the C.I.A., is enhanced by its unique legal status within the Federal Government. Unlike the Agriculture Department, the Postal Service or even the C.I.A., the N.S.A. has no specific Congressional law defining its responsibilities and obligations. Instead, the agency, based at Fort George Meade, about 20 miles northwest of Washington, has operated under a series of Presidential directives. Because of Congress's failure to draft a law for the agency, because of the tremendous secrecy surrounding the N.S.A.'s work and because of the highly technical and thus thwarting character of its equipment, the N.S.A. is free to define and pursue its own goals.

Despite the unpenetrable secrecy surrounding the agency

— its public budget or access to its premises is allowed — its mission was first discussed openly in the 1975 hearings of the Senate Select Committee on Security Government Operations with Respect to Intelligence Activities. Various aspects of the agency's responsibilities also have been touched upon in a handful of documents filed by the agency in Federal courts, several recent executive orders and a few aging documents found in the towering stacks of the National Archives.

According to these sources, the N.S.A. has two broad goals, one offensive, one defensive. First, the agency aggressively monitors international communications links searching for "foreign intelligence," intercepting electronic messages as well as signals generated by radio or missile launches. Second, the agency prevents foreign penetration of communications links carrying information bearing on "national security."

According to an unpublished analysis by the House Government Operations Committee, the N.S.A. may have employed 120,000 people in 1976 when armed-services personnel were included in the official count. (According to a letter from the Joint Chiefs of Staff, overseas listening posts numbered 1,000.) In comparison, the F.B.I. had one employee for every six working for the N.S.A. The House report also estimated that the agency's annual expenditures were as high as \$15 billion.

The Senate select committee's study of the N.S.A., one of the most extensive independent examinations ever made of the agency, was initiated in the wake of Watergate and the disclosure of other abuses by Federal intelligence agencies. During the course of the investigation, its chairman, Senator Frank Church, repeatedly emphasized his belief that the N.S.A.'s intelligence-gathering activities were essential to the nation's security. He also stressed that the equipment used to watch the Russians could just as easily "monitor the private communications of Americans." If such forces were ever turned against the country's communications system, Senator Church said, "no American would have any privacy left.... There would be no place to hide."

Over the years, N.S.A. surveillance activities have in-

dead included Americans who were merely stating their political beliefs. The agency first became involved in this more questionable kind of surveillance in the early 1960's when either Attorney General Robert F. Kennedy or the F.B.I. asked it to monitor all telephone calls between the United States and Cuba. This list of international calls was significantly enlarged during the Johnson Administration as Federal authorities became concerned that foreign governments might try to influence American civil-rights leaders. The N.S.A. gradually developed a "watch list" of Americans that included those speaking out against the Vietnam War.

According to the subsequent investigation by the Senate intelligence committee, a total of 1,200 Americans were targeted by the N.S.A. between 1967 and 1973 because of their political activities. The subjects — chosen by the F.B.I., the Secret Service, the C.I.A. and the Defense Intelligence Agency — included members of radical groups, celebrities and ordi-

nary citizens. When it appeared that Congress might learn about the eavesdropping, the surveillance halted.

The Senate intelligence committee also discovered a second illegal surveillance program, under which the N.S.A., and its military predecessors, examined most of the telegrams entering or leaving the country between 1945 and 1973. The program was abruptly halted in May 1975, a date coinciding with the Senate committee's first expression of interest in it.

The records obtained by the committee indicate that from the project's earliest stages, both Government officials and corporate executives understood that the surveillance flatly violated a Federal law against intercepting or divulging telegrams. Certainly, they were aware that such interception violated the Fourth Amendment, guaranteeing against unreasonable searches and seizures, which also holds that a court warrant can be issued only when there is probable cause to believe a crime has been committed.

Using the information thus

gathered, the N.S.A. between 1952 and 1974 developed files on approximately 75,000 Americans, some of whom undoubtedly threatened the nation's security. However, the agency also developed files on civil-rights and anti-war activists, Congressmen and other citizens who lawfully questioned Government policies. For at least 13 of the 22 years the agency was building these files, the C.I.A. had access to them and used the data in its Operation Chaos, another computerized and illegal tracking system set up during the Vietnam War. At its peak, the Chaos files had references to more than 300,000 Americans.

Several months after the hearing, the Senate intelligence committee issued a report that expressed great concern about both the N.S.A.'s activities and the failure of Congress and the Federal courts to comprehend them. "The watch-list activities and the sophisticated capabilities that they highlight present some of the most crucial privacy issues now facing this nation," the committee warned. "Space-

age technology has outpaced the law. The secrecy that has surrounded much of the N.S.A.'s activities and the lack of Congressional oversight have prevented, in the past, bringing matters in line with the N.S.A.'s capabilities. Neither the courts nor Congress have dealt with the interception of communications using the N.S.A.'s highly sensitive and complex technology." The committee recommended that Congress approve specific legislation spelling out the precise obligations and limitations of the agency.

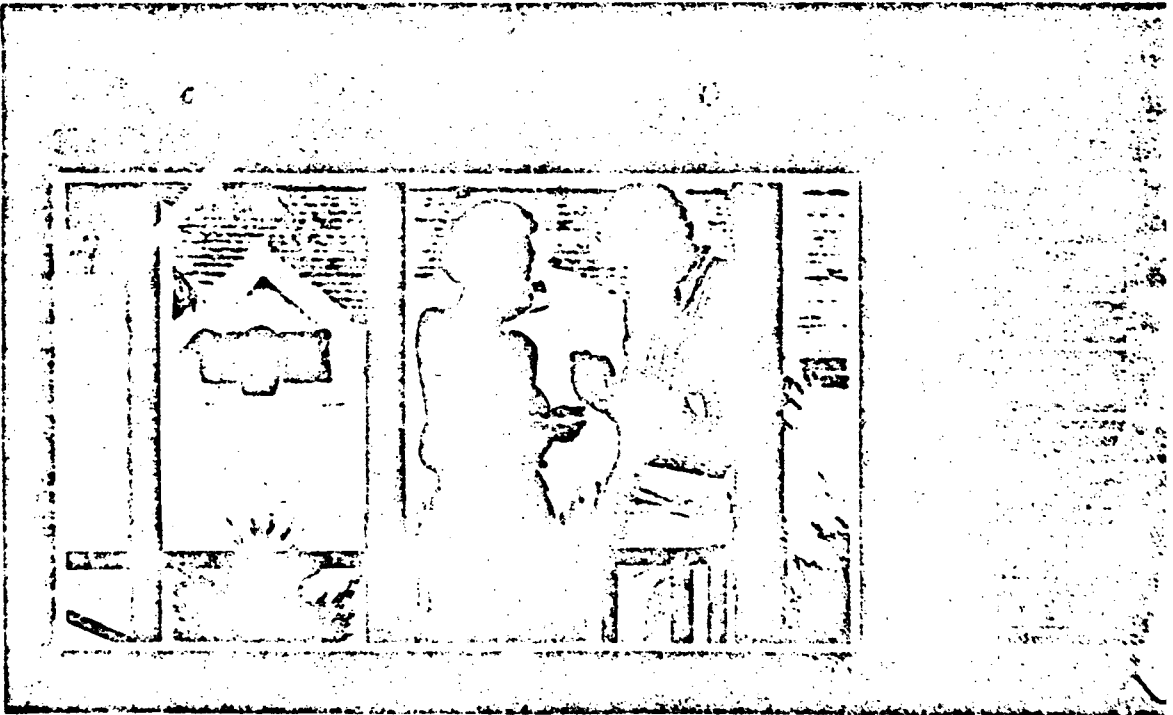
□

With the end of World War II and the start of the cold war, the value of effective intelligence remained high. In 1963, a special Presidential committee recommended the establishment of the N.S.A., replacing the four separate surveillance agencies within the Defense Department, concluding that a unified effort was essential because electronic surveillance of international communications "ranks as our most important

single source of intelligence today."

The logic of the cold war also dictated that intelligence include not only secret blueprints for the latest weapons or infiltrating the enemy's ranks with spies, but also early signs that a blight had hit China's rice crop, indications that a new oil field had been located in a remote corner of Russia and analysis of radio traffic at an important Soviet-bloc airport.

The already expensive aspects of American intelligence analysts was further sharpened by technical advances that were occurring, not entirely by chance, at the same time. The technology in question was the digital computer, the wondrous tool diligently developed by American scientists working for such companies as I.B.M., the RCA Corporation and Sperry Rand, and covertly underwritten in a major way by the N.S.A. The computers' ability to acquire, organize, store and retrieve huge amounts of data was an essential factor leading to the agency's enlarged definition of intelligence.



The Olga Plus with Lycra®

YOU'LL TAKE
A SHINE TO
BODYSILK HIGHLIGHTS™

Light up your under-16 in Olga's latest innovation a shimmering sensuous stretch fabric created by adding sheer Highlights to her sleek Bodysilk blend of soft nylon/Lycra® spandex. Olga's Bodysilk Highlights style #336 features light front-close underwire adjustable strap, 34-36 BC, 34-36 D. In light, sporty Champagne at 13.00 and D at 14.00 in the best Bra Departments.
*DUPRE registered trademark.

available at
B. Altman & Co., All Stores
and other stores with fashion sport



behind every
OLGA
there really is
an Olga



The importance of the broadest possible intelligence gathering became even more critical when computer know-how began to spread beyond a technological elite based primarily in the United States to scientists in many nations. Simply stated, the spread of advanced computer skills and the related mathematical concepts meant that governments could reduce the chances that their top-secret messages would be intercepted and decoded, while at the same time increasing their ability to collect all kinds of economic and technical intelligence.

As a result of these changes, according to several United States officials, the intelligence apparatus of the Soviet Union began eavesdropping on millions of telephone conversations between Washington and New York and several other major cities in the early 1970's. Because of the unusual sensitivity of the subjects, however, the Federal Government did not exactly trumpet the news of the Soviet surveillance.

In 1977, about three years after this surveillance became known to the United States Government, the Carter Administration formally announced that the Russians were conducting wholesale eavesdropping from at least four locations in three different cities, New York, Washington and San Francisco. The targets of real concern were the Government, defense contractors and other large companies whose activities would contribute to Soviet collection of economic intelligence. Henceforth, classified information relating to national defense and foreign relations would be transmitted only by secure means. The Administration proposed the immediate purchase of an additional 100 "voice scramblers" for what is called the Executive Secure Voice Network. The central switching point for the network was determined to be the N.S.A., a fact that was unacknowledged by the Administration.

President Carter's decision immediately broadened the category of information requiring Government scrutiny and significantly extended the authority of the N.S.A. Yet no unclassified document defines what kinds of information would be useful to an adversary. A timetable of the trains running between Washington and New York could be useful to an enemy spy. Newspaper articles

could serve as source material for intelligence operatives all over the world. Certainly, precedent had been established in 1971, when the N.S.A. was the lead agency in the Nixon Administration's attempt to stop newspapers from printing the Pentagon Papers, the bureaucratic history of the war in Vietnam. After blocking publication for 15 days, the Supreme Court ruled that the Government had failed to show why the material should not be published and that "without compelling reasons" prior restraint would be an unconstitutional infringement of the freedom of the press.

Until that time, the Federal Government sought to control and protect only those military and diplomatic secrets that had been declared confidential, secret or top secret under a long-established and formally prescribed classification procedure. But now, President Carter had decided to create a huge new category of material worthy of Government protection: information that "would be useful to an adversary."

Telephone links in the areas where Soviet spies were known to be listening were routed via underground cable. To further reduce the leakage of the new category of information, the President directed the N.S.A. to approach large corporations and other institutions, collect information about their communications networks and assist them in safeguarding their material.

□

The Carter directive sanctioning the N.S.A.'s involvement in the planning, organization and development of private communications systems not handling classified secrets was only one of several ways in which the power of the agency grew. Within the last few years, for example, the N.S.A. has forcefully moved to control the development and dissemination of inventive approaches intended to help the individual citizen, corporation or political organization maintain privacy.

On April 21, 1978, George I. Davida, then professor of electrical engineering and computer science at the University of Wisconsin at Milwaukee, received an order to keep secret all details of his invention, a computer security device. The N.S.A. informed Davida that under a little-known provision of the patent law a violation of the order could subject him to up to two years in jail and a

WJ

\$50,000 fine. The only problem was that Davida already had violated it by sending details of his invention to the National Science Foundation, one of the sponsors of his research, and a number of his academic colleagues. On the same day Davida received his secrecy order, the N.S.A. also obtained one on a patent application for a voice scrambler that would let radio

and telephone users talk without being overheard. The investors, Carl R. Nicola, William M. Raibe and David L. Miller, responded with a public statement, charging that the restraint appeared to be "part of a general plan by the N.S.A. to limit the privacy of the American people. They've been bagging people's purses for years, and now someone

comes along with a device that makes this a little harder to do, and they oppose this under the guise of national security."

After the agency's orders were publicized by several newspapers and magazines, the N.S.A. decided to pull in its horns. Inman, the N.S.A.'s director, told a House committee that the two orders exemplified "not a

fully law but inadequate Government attention to its application." He characterized the agency's handling of the voice-scrambling equipment as a "well-meant attempt to hold the line ... and clearly already been passed by."

A few years before, the director of the National Science Foundation, Richard C. Atkinson, and Inman had begun privately discussing whether the role of the spy agency in supervising cryptographic research should be expanded. The precise outcome of the talks remains murky, but the N.S.A. apparently won the debate. Today, the National Science Foundation routinely allows the N.S.A. to review any request for the funding of cryptographic research. The N.S.A. also has begun providing financial support for related unclassified civilian research. The first recipients of such support were two Stanford professors of electrical engineering, John T. Gill Jr. and Martin E. Hellman, a code expert who for many years had been sharply critical of the N.S.A.

"Five years ago, I was very much on the opposite side of the fence from N.S.A.," said Hellman. "I wouldn't say I have been co-opted. As a result of them being more friendly and coming part way I felt I should be more friendly. I guess I am now the first guinea pig."

Hellman is not sure why the agency was interested in funding nonclassified research, and he acknowledges potential problems. "One of the fears is that they are trying to buy people. If they support you, then they own you, and you really are going against them if they ask you not to publish something ... do you do?"

There are, of course, many ways to influence men. In early 1979, Inman spoke to the Armed Forces Communications and Electronics Association, the first public speech ever given by a top N.S.A. official. Speaking in the guarded language of his profession, Inman noted that the agency's mission could "no longer remain entirely in the shadows." One reason for this change, he explained, was that the protection of communications was no longer of interest just to the Government; it also had become a major concern to private institutions. Because of this new interest, tensions, which he did not define, had developed between "the national-security interests of the Government and the telecommunications-security interests of both the public and private sector." The time had come, he said, to begin a dialogue between the N.S.A. and the academic and industrial worlds.

The result of this dialogue so far has been the recommendation by a special committee of the American Council on Education, a prestigious organization of over 1,000 colleges and universities, that all researchers engaged in cryptographic research submit their work to the N.S.A. before publication. Only one of the nine members of the special committee opposed this "voluntary" system of prior restraint, George Davida.

Davida, who believes such a system



"For a business couple like us, pressured and played out, Bermuda is very special."

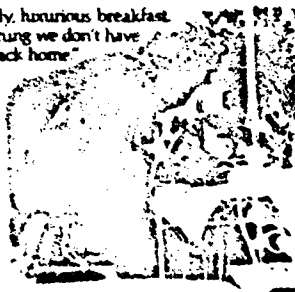
Sylvester and Nancy Gardiner talk about their second visit to Bermuda.



"There's incredible beauty here. We relax, we're restored, we find time for one another."

"A leisurely, luxurious breakfast. It's the one thing we don't have in our lives back home."

Couldn't you use a little Bermuda right now?
Bermuda



See your travel agent or write Bermuda, 2077-1000, Suite 200, 2700 Ave. of the Americas, New York, N.Y. 10017. In Bermuda, write Bermuda, P.O. Box 1000, St. John's, Bermuda. In Canada, write Bermuda, P.O. Box 1000, Toronto, Ontario. In Europe, write Bermuda, P.O. Box 1000, London, U.K. 20003.

is unconstitutional, said. "The increase in the computerization of society has led to the construction of a large number of data bases that are 'electronic windows' into the most intimate details of people's lives. What is even more disturbing is that it is usually impossible to know who is looking in. Thus, these data bases are like one-way mirrors."

"Encryption," he continued, referring to the coding of material placed in computers, "can serve as a curtain. Therefore, the need for civilian (or nongovernmental) effort in cryptography is a strong one."

Davidson noted that the data bases used right now for statistical purposes, employment records, credit-card operations and many other operations essential to American life are all subject to possible N.S.A. scrutiny. "The only effective method for

maintaining separation of such data involves encryption," he declared.

Shortly after Inman presided the academic community to accept his system of prior restraint for cryptology. He was named Deputy Director of Central Intelligence by President Reagan, who replaced him with Air Force Lt. Gen. Lincoln D. Fournier. (Later, Inman left the C.I.A. to become the director of the Microelectronics and Computer Technology Corporation, a private consortium of 10 high-technology companies.) Inman soon warned that many researchers would face mandatory Government censorship of their papers unless a system of review was established to limit the access of the Soviet Union to the benefits of American technology.

Speaking before the annual meeting of the American As-

sociation for the Advancement of Science last year, Inman said that other areas where restrictions were required because publication of certain "technical" information could affect the national security in a harmful way. Examples include computer hardware and software, other electronic gear and techniques, lasers, crop projections and manufacturing procedures.

Many scientists immediately objected. "If you want to win the Indianapolis 500, you build the fastest car; you don't throw nails on the track," commented Peter J. Denning, head of Purdue University's Department of Computer Sciences and former president of the Association for Computing Machinery.

The American Association for the Advancement of Science passed a brief resolution in the day Inman spoke:

"Areas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and the scientific process, so it resolved that the A.A.S. opposes governmental restrictions on the dissemination, exchange or availability of unclassified knowledge."

A few months before Inman's speech, Dr. Edward Teller, the physicist credited with being a major proponent of and contributor to the construction of the hydrogen bomb, wrote an essay attacking Government attempts to restrict scientists, saying, "Secrecy is not compatible with science, but it is even less compatible with the democratic procedure."

No laws define the limits of the N.S.A.'s power. No Congressional committee subjects the agency's budget to a

systematic, informed and skeptical review. With unknown billions of Federal dollars, the agency purchases the most sophisticated communications and computer equipment in the world. But truly to comprehend the growing reach of this formidable organization, it is necessary to recall once again how the computers that power the N.S.A. are also gradually changing lives of Americans — the way they bank, obtain benefits from the Government and communicate with family and friends. Every day, in almost every area of culture and commerce, systems and procedures are being adopted by private companies and organizations as well as by the nation's security leaders that make it easier for the N.S.A. to dominate American society should it ever decide such action is necessary. ■

EXCLUSIVELY
OURS THE
MARSHALLFIELD
CHAMBERSTICK
CASTS AN
ELEGANT GLOW

Marshall Field's

Marshall Field's COUPON
CHICAGO, ILLINOIS 60611

Name _____
Address _____
Phone _____

Credit please send to Marshall Field's Co. Inc. Checkoff the amount of my bill

Please I prefer Marshall Field's Marshall Field's Marshall Field's

By _____ Date _____



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: N0832
14 June 1983

The Honorable Glenn English
Chairman, Subcommittee on Government
Information, Justice and Agriculture
Committee on Government Operations
United States House of Representatives
Room B349B Rayburn House Office Building
Washington, D.C. 20514

Dear Mr. Chairman:


This letter responds to your letter of May 5 1983, to me concerning the New York Times article of Thursday, April 28, 1983 about the visit and actions of representatives of this agency to the George C. Marshall Research Library. I will attempt to address your questions about the events reported in the article.

The Marshall Library has a government-authorized secure storage facility and government-approved security clearances for archivists to permit the Library to hold classified and otherwise sensitive government-originated information contained in the collections entrusted to it. The Library holds the collections of two former National Security Agency officials: former NSA Director, LTG Marshall S. Carter (who is currently the President of the Marshall Foundation, the Library's parent organization) and Mr. William F. Friedman, a former cryptologist at NSA. Both of these collections contain some classified and otherwise sensitive information.

The NSA and the Marshall Library have had a long and mutually beneficial working relationship which has, among other things, involved the declassification by NSA of much information contained in the Friedman collection as well as the provision by NSA to the Library of related historical material and the loan of certain government-owned equipment. This relationship has resulted in what we believe to be the best possible means of making the maximum amount of this material available to the public for historical research while at the same time protecting valid national security-related information as required by law.

Enclosed are our answers to your specific questions. Also enclosed is a copy of a letter to General Carter asking his permission to review his collection. You had requested copies of the correspondence between NSA and the Library in your letter. This correspondence is dispersed throughout the Agency. It is taking some time to pull this together. We will provide copies of this correspondence as soon as possible.

Sincerely,


LINCOLN D. FAURER
Lieutenant General, USAF
Director, NSA/Chief, CSS

Encls:
a/s

RESPONSES TO QUESTIONS FROM REP. GLENN ENGLISH

"1) What prompted NSA to review the papers at the Marshall Library?"

NSA's most recent review of materials at the Marshall Library was occasioned by revelations in the book, The Puzzle Palace, by V. James Bamford. The book disclosed certain information obtained from the General Marshall S. Carter and William F. Friedman collections at the Library.

We concluded that the papers of General Carter, a former Director of NSA, should be reviewed because they could contain sensitive information, i.e., information which is classified, classifiable, or otherwise protected pursuant to statutory authority, derived by him as a result of the conduct of his duties as Director. It was necessary, therefore, that his papers be reviewed to ensure that the materials were properly identified as those which are classified/protected information and those which could be made fully available to the public. Before conducting a review of the Carter collection we sought General Carter's permission to do so (the Carter collection had been closed after the publication of The Puzzle Palace). General Carter granted NSA permission to conduct a review of his collection at the Library and also advised NSA that it had been his intention all along that his collection be closed to all but the General George C. Marshall biographer.

We had reviewed the Friedman collection from time to time since it was first provided to the Library in 1970 for purposes of declassification of information where possible and also to confirm the sensitivity and assumed removal from public access of other information it contained. Bamford's book made reference to materials in the Friedman collection that NSA had understood, based on a previous review, to be closed to the public.

"2) Which collections were reviewed and how were they selected for review? When were the reviews conducted?"

The Friedman and Carter collections were both reviewed for the reasons set out in the response above. No other collections were reviewed because we knew of no other collections that might contain any sensitive information related to NSA. The reviews took place on April 4-7, 1983.

"3) Which papers were reviewed and how were they selected for review?"

The review focused on the correspondence files of William Friedman and those files of the Carter collection concerning his years at NSA.

The Friedman correspondence files were selected because references to these files in The Puzzle Palace indicated that these files were open to the public. As noted, NSA had had an explicit agreement with the Library that portions of the Friedman correspondence which continue to be sensitive would be closed to the public. This agreement was an outcome of a prior review of the Friedman collection conducted by NSA. NSA learned at the April 1983 review of the Friedman collection that a former archivist of the Library had opened the collection to the public without obtaining the approval of the Library's authorities or advising NSA of his intention to open these papers to the public.

The files in the Carter collection relative to his years as Director, NSA, were chosen for review because they were likely to contain information General Carter derived from his conduct of official duties at NSA.

"4) Does NSA have any ownership or other rights with respect to any papers in the Marshall Library Collection?"

There are some materials on loan to the Marshall Foundation from NSA for which the Government maintains a right of ownership. Additionally, all information which is derived from the performance of governmental functions which is classified, classifiable, or unclassified but protected against disclosure by statute, may be protected by the government until such time as that information is officially declassified or the government otherwise indicates that the information is required to be protected. NSA is responsible for ensuring the protection of such information when it concerns NSA activities. The authority underlying NSA's responsibilities is briefly discussed in the answer to paragraph 8, infra.

"5) The New York Times reported that some papers were withdrawn from public files at the request of NSA."

"a) Were any of the papers reviewed by NSA already classified? Had any of the papers been declassified?"

Some of the papers reviewed were already classified. Some of the materials in the Friedman collection which were reviewed by NSA representatives in April had been declassified during previous reviews by NSA. No materials from the Carter collection had been declassified since there had been no previous reviews of that collection.

"b) Did NSA classify any papers in the Marshall Library? If so, how many pages were classified? On what authority were these papers classified? Please be specific with respect to the classification rules in Executive Order 12356."

One technical monograph in the Friedman collection which had been previously declassified was found to contain infor-

mation which, if disclosed, could cause damage to the national security and, thus, should have been maintained in a classified status. There was no indication at the time of the review that this document had been disclosed to the public in fact. The section of Executive Order 12356 governing this action is Section 1.6(c).

In addition to this monograph, some other documents in the collections were marked by the NSA representatives as classified or, in the case of one document, had its existent classification marking upgraded. The documents were marked or upgraded pursuant to Executive Order 12356, Section 1.3.

We did not maintain a record of how many pages were marked as classified.

"c) Were any papers marked 'For Official Use Only'? If so, how many? What is the significance of the designation 'For Official Use Only'?"

Several papers in the collections contained information of a kind which should be marked "For Official Use Only". Information marked "For Official Use Only" is a kind which has not been given a security classification pursuant to the criteria of a classification Executive Order, but which may be withheld from the public for one or more reasons cited in Exemptions 2 through 9 of the Freedom of Information Act (FOIA). The principal basis of NSA's use of this marking is to designate information permitted to be protected by Section 6 of The National Security Agency Act of 1959 (50 U.S.C. §402 note, Public Law 86-36). This statute protects information related to the functions, activities, and organization of NSA as well as certain information concerning its personnel. This statute operates to trigger the applicability of FOIA exemption 3 which provides for the exemption from disclosure under the FOIA information specifically protected by statute.

Of the materials identified in the review as containing such information some were marked as "For Official Use Only", but a specific count of those materials was not kept. It was recommended to the Library officials that all the materials identified as "For Official Use Only" be kept closed to the public.

"d) Did NSA request that any unclassified papers be removed from the public files? If so, why?"

At the time the NSA representatives conducted their review in April, the materials were located in the secure vault, i.e., a place closed to the public. The Carter collection had been closed to the public prior to NSA's review. It was not known, at the time of the review, which papers had previously

been open to public view or which papers had actually been viewed by the public. NSA representatives did request that the materials identified as containing classified information or information "For Official Use Only" be kept closed to the public because the materials so identified required protection pursuant to the authorities already cited.

"e) Did NSA physically remove any papers from the Marshall Library collection?"

No.

"f) Library officials told the New York Times that NSA requested that some documents should be put in a vault. Why?"

As noted, all the materials reviewed were already in a vault at the time of the review. The request that certain materials be kept closed to the public amounted to a request that these documents remain in the vault - an action already taken by the Library.

"g) On what basis did NSA determine that some papers in the Marshall Library collection should be treated as if they were classified, placed in a vault, or simply removed from public access?"

Both Executive Order 12356 and Public law 86-36 applied to the classified and sensitive materials, respectively, as set out in our responses to questions 5b and 5c, above.

"6) Did NSA review the security arrangements at the Marshall Library to determine if they afforded sufficient protection for information deemed to be sensitive? Did NSA ask the Library to restrict access to individuals approved by NSA or individuals with security clearances?"

The security arrangements, clearances and facility at the Marshall Library were established and are certified by the U.S. Army. NSA accepts the Army's determination as adequate. Such arrangements presuppose restricting access to classified materials to cleared individuals. NSA made recommendations to the Library that certain materials be maintained as closed to the public.

"7) The New York Times article quoted a letter from you to Marshall S. Carter as stating that the visit to the Marshall Library by NSA officials was 'part of a continuing review of research materials used by author James Bamford'."

"a) What is the nature and extent of this review?"

After the publication of The Puzzle Palace, a review of the source material cited by the author was undertaken by

NSA. This review was commenced in order (i) to identify classified or otherwise protected information compromised in the book, if any; (ii) to take all appropriate security countermeasures, if any compromise had occurred; (iii) to identify any unauthorized disclosures appropriate for further investigation; and (iv) to gather information pertinent to assessments of current information security practices. This review process was almost entirely limited to a review of documents cited by the author. No institutions other than the Marshall Library were contacted and no documents were requested to be removed from public access as a result of this review except those found in the Friedman and Carter collections which were enumerated in our answers to question 5, above.

This review was consistent with our responsibility to ensure the protection of information relating to cryptology that is derived from the performance of official duties. As part of its routine responsibilities and functions, NSA conducts reviews of published information to determine if classified or protected information has been improperly disclosed.

"b) What other institutions or individuals have been contacted by NSA as part of this review?"

Only former NSA employees and officials have been contacted as part of our review effort. No other institutions have been contacted.

"c) Has NSA requested that other papers be removed from public access? Please describe any such requests."

Our reviews stemming from the publication of Bamford's book have not caused us to make any such requests of any individuals or organizations except the requests of the Marshall Library.

"d) Are there any other ongoing or completed reviews of materials other than those used by James Bamford?"

As part of our responsibility to protect classified and sensitive information related to NSA's operations, we frequently review materials intended to be published - often at the explicit request of an author.

"8) Does NSA have any authority to classify information in private papers? From what provision of law or Executive Order does this authority derive?"

The papers in the Friedman and Carter collections deemed to be classified are those containing information about NSA functions and activities derived from their official duties with the

Agency that is classified under Executive Order 12356. NSA officials exercise classification authority under Executive Order 12356, as implemented by DoD Directive No. 5200.1, as the agency or successor agency having cognizance of the cryptologic functions and activities involved.

Under 18 U.S.C. 798(b) the Secretary of Defense may determine the persons authorized to receive classified cryptologic information. Under Executive Order 12333--as under predecessor orders--the Secretary of Defense conducts, as the executive agent of the United States Government, signals intelligence and communications security activities. The same order authorizes the National Security Agency to execute the Secretary's responsibilities to conduct signals intelligence and communications security activities, and authorizes the Agency to protect by appropriate means signals intelligence and communications security information within its cognizance. Further, Section 6 of the National Security Agency Act of 1959, authorizes NSA to protect from disclosure information regarding the organization, functions and activities of NSA and the persons employed therein.

The law recognizes that the U.S. Government, through NSA, may properly seek to protect information and data of the kinds within the ambit of the statutes and Executive Orders cited above, when such information is derived or acquired through an affiliation with the Government - regardless of whether the information is contained in official or private papers. The law also recognizes that individuals provided access to such information, i.e., individuals placed in positions of trust and confidence in respect to the Government, have a fiduciary obligation to prevent the disclosure of such information or data outside the channels authorized by the government. Snepp v. United States 444 U.S. 507 (1980). Individuals affiliated with NSA sign secrecy oaths in which they explicitly accept and acknowledge their obligations regarding protected information and data acquired through association with NSA.

"9) Does NSA have any authority to restrict disclosure of information in private papers if the information is not subject to classification under Executive Order 12356?"

The authority of NSA under Section 6 of the National Security Agency Act of 1959 to protect against disclosure information, derived from the conduct of official duties, about its organization, functions, activities, and personnel is not limited to classified information or information contained in official documents. It applies as well to information of those kinds that is classifiable but not yet formally classified under Executive Order 12356 and to other information that meets the statutory criteria for protection.

"10. Had NSA examined any of the materials at the Marshall Library before learning of James Bamford's plans to publish a book on NSA?"

Yes. NSA and the Marshall Library have had a long and mutually beneficial working relationship dating back to our assisting in the transport of the Friedman collection to the Library in 1970. Marshall Library officials have long looked to NSA representatives to periodically review documentation in the Library. This review serves not only to ensure that classified or sensitive information is properly protected, but also to declassify as much of this information as possible so that the interests of the Library, the Marshall Foundation and the public can best be served.

"11) Has NSA ever provided any funds to the Marshall Library? Is NSA now considering providing any funds to the Library?"

No funds have been provided to the Library, nor is it anticipated that any will be.

"12) Did William F. Friedman enter into a secrecy or pre-publication agreement with NSA, its predecessor organization, or with any other government agency? If so, please provide a copy."

We can only answer this question as it relates to NSA and its predecessor organizations. It is believed William F. Friedman signed a secrecy oath similar to that signed by all employees of this agency and its predecessor organizations. All records which would include Mr. Friedman's oath have been retired. We are attempting to retrieve a copy of that oath for you and will provide it to you when it is available.



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755


Serial: N0352
17 March 1983

Lieutenant General Marshall S. Carter, USA (Ret)
655 Bear Paw Lane North
Colorado Springs, CO 80906

Dear General ^{Pal} Carter:

I appreciated your coming up to Denver last month so that we could talk. It is obvious that we share a common desire that collections of papers not be exploited unreasonably by researchers to expose classified or sensitive information, although this is often difficult to enforce. As a part of our continuing review of research materials used by author James Bamford, Mike Levin, Chief of the Information Security Division, and Russ Fisher, of our Archives and History Office, propose to visit the George C. Marshall Research Foundation during the period of 6-8 April 1983 and would like very much to take this opportunity to review your papers. The review would be for potential classification and historical reference purposes but obviously requires your approval since your files are closed. They will also be taking another look at the William Friedman collection. We would, of course, share with you the results of our review.

Sincerely,


LINCOLN D. FAURER
Lieutenant General, USAF
Director, NSA/Chief, CSS

Southam News Services

Prairie Bureau
~~FROM AMK/ED/MAK~~
 502 Herald Building,
 206 7th Avenue S.W.
 Calgary, Alberta T2P 0W7
 Tel: (403) 266-2245

Bureaux in:
 Ottawa, Montreal,
 Toronto, Vancouver,
 London, Washington,
 Paris, Nairobi.

28 October 1983

Rep. Robert W. Kastenmeier
 Chairman
 Subcommittee on Courts, Civil
 Liberties and the Administration
 of Justice
 Room 2137B
 Rayburn House Office Building
 Washington, D.C. 20515
 U.S.A.

Dear Mr. Chairman:

As you may already know, I have declined an invitation to appear before your subcommittee Nov. 2 in Washington, D.C. There are several reasons for my non-appearance, including the fact I am a Canadian citizen who feels he ought to play no direct role in the U.S. legislative process.

In addition, my recent experience as the target of a U.S. Federal Bureau of Investigation intelligence inquiry in connection with my duties in Washington, D.C. as a reporter for Southam News has been capably, accurately and fairly reported in segments of the American, Canadian and British press.

Anything I could add now about the episode would probably be redundant, leaving me open to criticism that I'm a promoter for myself -- or worse, a reporter who flogs old news.

Moreover, any solutions to American freedom of speech or press issues raised by my case lie in the hands of concerned Americans, not foreign-based journalists such as myself.

I would, however, be remiss if I did not tell you

...2

that the experience with the F.B.I. and the U.S. Justice Department caused considerable anxiety among my friends and family. Certainly, the episode darkened the final two months of my four-year assignment in Washington, and placed me under a cloud of suspicion and innuendo.

It is, of course, flattering for any reporter to discover that he or she has caused unease somewhere in a government by exposing a dirty little secret or by illuminating a subject of public interest. This happens routinely in Washington, where an army of journalists works relentlessly to reveal the damning facts, often aided by courageous informants inspired by a sense of public duty.

But in my case, the flattery accorded my work consisted of a business-like telephone call from an F.B.I. agent who invited me in for what seemed a mandatory discussion at the Washington, D.C. Field Office, Buzzard Point. I can assure you it's no picnic when two F.B.I. agents ask you to name your sources, and then ignore your request for clarification of your status in their interview room.

There is also little joy three weeks later when you hear an officially-spread rumor that you are facing imminent indictment by a federal grand jury. Equally worrisome is the knowledge that your copy transmissions by computer and long-distance telephone can be legally intercepted and monitored by the National Security Agency. And when you catch the NSA at it one day, there is only a curt "no comment" from the agency. Forgive me, but this seems an abuse of technology that is unworthy of the United States. For 25 cents, the United States Embassy in Ottawa could obtain the same information, albeit a day or two later, when it's published by the Ottawa Citizen.

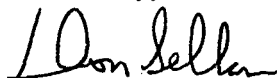
Throughout my experience, I was left to wonder whether the United States government was sending a message to me, or simply trying to frighten the sources of my information. Talk by U.S. Justice officials of possible Espionage Act or Theft-of-Government-Property Act charges has a chilling effect on the entire information process.

At one point, I suddenly wondered whether the time had come to inject a more diplomatic tone into my writings about events in Washington. Fortunately, this silly temptation lasted about 30 seconds and vanished, unfulfilled. The more general atmosphere of intimidation remained, however, until my family returned to Canada in mid-summer.

Today, I am free to consider from afar the plight of my informants who remain in the U.S. and who must try to live in that intimidating climate. I often think about public servants who are confronted by the increasing threat of polygraph tests whenever a secret tumbles out of the bureaucracy and onto a front page or a TV screen.

And when I do, I wonder what, if anything, anyone will do about it.

Yours truly,



Don Sellar,
Prairie Correspondent
Southam News of Canada

FBI Quizzes Canadian Correspondent About Source of Defense Information

By Howard Kurtz

Washington Post Staff Writer

When Donald Sellar, Washington correspondent for Canada's largest newspaper chain, was called by the FBI in June, he was more than a little concerned.

Sellar knew that officials in the U.S. intelligence community were upset about his articles for the Southampton Inc. chain on Pentagon weapons testing. But he said he had not expected to be questioned by two FBI agents, who asked him to identify the source of his documents.

"It became immediately evident that they were not just trying to track down leakers, they were investigating me," Sellar said.

The incident highlights the Reagan administration's determination to crack down on unauthorized leaks. Concern about that was underscored yesterday by disclosure that President Reagan warned federal employes Tuesday that they could be prosecuted for disclosing classified information.

The FBI interview of Sellar was approved by Attorney General William French Smith. It was followed by a newspaper report that the Justice Department was considering seeking an indictment of Sellar, a Canadian citizen, under a statute dealing with theft of government property. This prompted complaints from the Canadian Embassy and media.

Justice and FBI spokesmen would neither confirm nor deny that Sellar is or was under investigation. Justice spokesman Mark Sheehan said department guidelines require the attorney general to approve all questioning of reporters.

Sellar, 37, who has returned to Canada, caused a stir with a report in October about secret negotiations to allow U.S. testing of cruise missiles and other weapons in Canada.

The day after he filed the story by computer transmission over a telephone line, an intelligence source

warned him that U.S. officials were upset and that "there was a witch hunt under way for my sources," Sellar said.

Sellar said he was disturbed even more that the source quoted at length from the article, even though it had not yet been published. Sellar later reported that the National Security Agency apparently had intercepted his transmission of the story.

When FBI agent Douglas Gregory requested an interview, Sellar said,

Gregory noted that Sellar had a White House press pass. Sellar said he wondered whether his credentials were in jeopardy.

Sellar said he refused to tell the FBI his sources for several military stories. He said they showed him the cover sheet of a classified document called "Air Force 2000," a military planning paper about which he had written, and asked whether he had obtained a copy from a federal employe. Sellar said he told them he had not.

The agents then asked if he had met with any Soviets, Sellar said. He said he told them two reporters had invited him to lunch with a reporter

for the Soviet newspaper Izvestia. "They [the agents] were either trying to send me a message or send a message to my sources," Sellar said.

"If this had happened in Canada to an American journalist," he said, "there would be a huge public outcry in the U.S."

"We had to register our concern on this," said Patrick Gossage, the Canadian Embassy's information minister. "We were very concerned about a Canadian national being investigated for an alleged possession of documents that also were in the hands of American reporters. Why pick on a Canadian when these things go on all the time?"

CHRONICLE

The FBI bears down

On a Saturday night last October, Donald Sellar, the lone Washington correspondent for Canada's biggest newspaper chain, Southern Inc., received an unusual phone call from one of his sources in the intelligence community. The source warned Sellar that a story he had written the previous day concerning negotiations between the United States and Canada for an agreement to test the cruise missile in Canada was causing quite a stir in Washington and that a hunt was on for his sources. The caller said that the story was already being circulated in defense and intelligence circles, and he quoted comments from the piece to convince Sellar that he had seen the actual article. What troubled Sellar was that the story had not been published yet and would not appear in any Canadian paper for another thirty-six hours.

Like many foreign correspondents, Sellar transmits his stories to his home bureau over international telephone lines. He soon learned these could be monitored by the National Security Agency, and the next week he wrote a story about how the NSA was apparently intercepting Southern copy. In the months that followed, Sellar continued to report on the secret cruise-missile testing negotiations — a story he had broken in March 1982, which had spurred vigorous antimissile protests in Canada and had confronted the government of Prime Minister Pierre Trudeau with political problems.

But for more than a year, Sellar had no idea that his stories were causing any more anxiety in the Reagan administration than those of countless other Washington reporters who routinely deal in brown envelopes. Then, last June 8, he received a "very businesslike" call from FBI agent Douglas Gregory. "He said he was working on an intelligence investigation, and he wanted to talk to me," says Sellar, a native of Alberta who started his reporting career at the *Calgary Herald* before moving to Southern's Ottawa bureau in the early '70s. Agent Gregory refused to disclose the purpose of the interview, saying it would become "immediately obvious to me when we had our meeting." Sellar recalls, Gregory suggested that Sellar come to the Old Executive Office Building next door to the White House. add-

ing, "You do have a White House pass."

Sellar inferred that his coveted White House credentials might be jeopardized if he refused to cooperate. He decided to comply with the request and suggested that the agents come to his office. They refused, asking instead that Sellar come to the FBI's Washington field office. A half-hour later, Sellar recalls, he was escorted into an interview room by Gregory and a second FBI agent. After a few minutes of small talk, Sellar says, the interview went as follows: Gregory pulled out the cover sheet of a classified document, titled "Air Force 2000," concerning long-term military strategic planning. Asked if he had seen the document, Sellar replied that he had written a story about it. The agents asked if his source was a U.S. government employee, and Sellar said no. They asked who had given Sellar the document, and he refused to tell them. The agents then asked if Sellar had written anything about the cruise missile. Sellar laughed, knowing that the agents must have been well aware of his stories. The agents pressed him further on the cruise stories and then abruptly changed the subject, asking about any contacts he might have had with "a Soviet." Yes, Sellar responded, a few weeks earlier, he and two other Canadian journalists had lunched with *Izvestia's* Washington bureau chief. The interview then ended.

In the weeks after the interview, the Justice Department confirmed that Attorney General William French Smith had personally approved the FBI's decision to question Sellar, and other sources revealed that the investigation was aimed not just at locating Sellar's sources but also at Sellar. Nearly all previous leak investigations have focused exclusively on leakers rather than the reporters who disclosed the information. But in this case the Justice Department was considering seeking an indictment of Sellar himself under a statute dealing with theft of government property. Both the FBI and the Justice Department have repeatedly refused to comment publicly on the investigation.

Although an indictment of Sellar is now regarded as highly unlikely — because of Canadian government protests and the

amount of press attention the story has received on both sides of the border — the investigation continues. Why did the U.S. government single out Sellar? One theory is that the Canadian government triggered the entire episode by suggesting that it might break off the missile-testing negotiations if the Washington leaks to Sellar were not plugged. In fact, according to a Defense Department document obtained late last June by Cox Newspapers, the U.S. State Department had asked Defense to look into the leaking of certain "classified/sensitive diplomatic information," and the resulting investigation began almost immediately after Sellar's first disclosure in March 1982.

The Defense Department, however, says that the 1982 leak listed in the memo does not involve Sellar. In addition, the Canadian government denies that it requested a formal investigation of the leaks or threatened to walk out of the negotiations, although it admits having expressed displeasure with Sellar's articles. "We were unhappy, and we made that known through the American embassy [in Ottawa]," says Patrick Gossage, Minister/Counsellor for Public Affairs at the

Sellar in Southern's Washington office



CHRONICLE

Canadian embassy in Washington. But an American official has a different interpretation of the Canadians' message. "It was put in nice diplomatic language that, given the various leaks, it would be very difficult to continue our negotiations fruitfully if you don't put the leaks to rest," he recalls. Whether or not the Canadian government meant to instigate an investigation of a Canadian foreign correspondent, it has acted swiftly on Sellar's behalf. Embassy officials have requested information about the reporter's treatment from both the State Department and the FBI, and at one point warned that an indictment would have a "deleterious effect" on U.S.-Canada relations. In the meantime, Sellar himself, who was reassigned to Canada at the end of July fol-

lowing his four-year tour of duty in Washington, has filed a Freedom of Information Act request for his FBI file.

Shortly before he left for home, Sellar was on the phone with Nicholas Hill, general manager of Southam News, who informed him that an influential Southam paper, the *Ottawa Citizen*, would soon be publishing an editorial objecting to his treatment. That night, Sellar received a call from one of his defense-community sources. The message: U.S. officials already knew that the *Citizen* would soon be publishing such an editorial.

Cheryl Arvidson

Cheryl Arvidson, a reporter in the Cox Newspapers Washington bureau, covered the Sellar story for Cox.

THE NEW YORK TIMES, THURSDAY, APRIL 28, 19

Security Agency Bars Access to Nonsecret Material, Library Records Show

By PHILIP TAURMAN

Special to The New York Times

WASHINGTON, April 27 — The National Security Agency, the nation's largest and most secretive intelligence organization, has directed a private library in Virginia to halt public access to personal letters mentioned in a book critical of the agency, according to library records.

In a visit to the George C. Marshall Research Library in Lexington, Va., earlier this month, according to library officials, two representatives of the security agency also put a "secret" rubber-stamp on some of the letters, which were written by a former agency official but were never Government property. Library officials said the security agency instructed them to place the letters, including many without the agency stamp, in a vault the library uses to house secret data.

Many of the letters were cited by the author James Bamford in his book "The Puzzle Palace," a critical report about the agency that was published last year. The National Security Agency is responsible for devising and keeping secure codes used by the United States, breaking encryption systems used by foreign governments and monitoring worldwide communications.

Removal Touted 'Routine'

Gen. Lincoln D. Fausch, director of the agency, defended the removal of the letters from public access, calling it a "routine" part of the agency's "responsibility to advise and assist in the protection of N.S.A.-related national security information" contained in library collections.

Scholars and civil liberties lawyers, asked this week about the agency's action, denounced it, in the words of one, as "a new form of censorship."

Mark H. Lynch, a lawyer for the

American Civil Liberties Union, said, "When the Government starts barring the public from seeing unclassified documents in private libraries, it's an extraordinary form of censorship."

Historians and lawyers said they had never before heard of a case in which open research materials mentioned in a published book were later classified secret or removed from circulation. They also questioned the N.S.A.'s authority to declare secret or otherwise influence the status of documents that were never the property of the Government. Officials of the security agency assert that it does have such authority to protect national security information.

Excessive Secrecy Charged

While they were at the Marshall library, N.S.A. officials told the library that the visit was part of a systematic effort to track down and, if necessary, remove from public circulation research materials about sensitive matters that were used in Mr. Bamford's book, library officials said.

Mr. Bamford is a Massachusetts writer who has a law degree and specializes in investigative research. "The Puzzle Palace," the first book-length account of the security agency's history and activities, accuses the agency of maintaining excessive secrecy and abusing its powers of electronic surveillance by spying on American citizens in the 1970's.

Mr. Bamford said the recent action would "have a very chilling effect on any historical researcher."

The letters removed from open library shelves were written from 1943 to 1969 by William F. Friedman, a pioneer in cryptological work in the United States and one of the security agency's top code breakers. They dealt primarily with personal matters, according to library officials.

The letters contained brief references

to some cryptologic work, including one project in 1957 that the agency still considers highly sensitive, according to Mr. Bamford's book, but were never subject to secrecy classification because they were part of Mr. Friedman's private papers. Mr. Friedman died in 1969 and donated his private papers to the Marshall library.

In a letter last month to Marshall S. Carter, a former director of the agency and president of the foundation that oversees the Marshall library, General Fausch described the visit by two N.S.A. officials as "part of our continuing review of research materials used by author James Bamford."

The letter also said, "It's obvious we share a common desire that collections of papers not be exploited unreasonably by researchers to expose classified or sensitive information, although this is often difficult to enforce."

Officials at the Marshall library, which is on the campus of the Virginia

Military Institute, called the agency's action "troublesome" but defended the library's relationship with the Government. "I've felt that our relationship with the Government has been reasonable, practical and helpful," said Fred L. Haduel, director of the George C. Marshall Research Foundation.

General Marshall, the Army Chief of Staff in World War II and later Secretary of State and founder of the European postwar recovery plan that bears his name, was a graduate of V.M.I.

Rogans Executive Order

Mr. Haduel said the foundation's relationship with the Government "is not and should not be an adversarial relationship," and added: "Collections come from different people under different circumstances and different conditions. We are trying, step by step, to move toward an equitable opening of all our collections."

An executive order on national se-

curity information signed by President Reagan last year limited the definition of information subject to designation as secret as material "that is owned by, produced by or for, or is under the control of the United States Government."

Mr. Hadsel said the library removed the Carter papers from open access last year. He declined to say why. Mr. Bamford, who interviewed Mr. Carter while doing research for his book, said the Carter papers were withdrawn at the request of Mr. Carter after publication of "The Puzzle Palace." Mr. Carter could not be reached for comment today.

Records at the Marshall library show that a number of papers from the Friedman collection were withdrawn from public files at the instruction of the security agency.

A reporter who asked Monday to see several of the Friedman letters mentioned in Mr. Bamford's book was given the relevant files of correspondence. The specific letters, however, were missing; in their place were notices that the documents had been withdrawn for security reasons. In some cases, entire folders had been withdrawn.

For example, Mr. Friedman's correspondence with Boris C. W. Hagelin, a European manufacturer of cryptologic equipment, was missing from the collection. In place of the folder was a one-page notice stating that that the material had been removed because it contained "security-classified information" and had been designated as "For Official Use Only" by the security agency. There are several references to the

Hagelin letters in Mr. Bamford's book.

Library officials said other material used by Mr. Bamford was stamped "secret" by the visiting security agency officials. Library officials said they had no choice but to remove the material from open circulation. "If something is classified, it's classified," one official said. "We have no choice but to remove it."

Other documents removed from the Friedman collection were marked by notices that made no mention of any security agency action. Library officials said these papers were not classified or otherwise officially designated as sensitive by the security agency. "They simply informed us that the papers were sensitive and told us to put them in the vault," a library official said.

Removal Viewed as Pointless

Several scholars said that, apart from any questions of censorship, removal of the papers seemed pointless because the material was published in Mr. Bamford's book. In addition, Mr. Bamford said, he kept copies of all the Friedman letters he used and would make them available to anyone who asked to see them.

"The removal doesn't make any sense from the standpoint of reason, let alone scholarship," said Samuel R. Gammon, executive director of the American Historical Association.

General Faurer said publication of the information did not matter. "Just because information has been published doesn't mean it should no longer be classified," he said.

APPENDIX.

THIS BOOK AND THE SECRECY AGREEMENT

The secrecy agreement that I signed when I joined the CIA allows the Agency to review prior to publication all writings of present and former employees to ensure that classified information relating to national security is not revealed. This provision seems logical and necessary to protect legitimate secrets. However, my experiences in getting this book approved show that the CIA uses the agreement not so much to protect national security as to prevent revelations and criticisms of its immoral, illegal, and ineffective operations. To that end, it uses all possible maneuvers, legal and illegal. Had I not been represented by my attorney, Mark Lynch of the American Civil Liberties Union (ACLU), and had I not developed a massive catalogue of information already cleared by the Agency's publications review board (PRB), this book could not have been published. The review of my manuscript came in two basic stages, first on an initial manuscript that I wrote without editorial assistance, and second on a revised manuscript written following an editor's advice.

On February 26, 1980, I submitted the first version of the manuscript to the Agency for review and on March 21, several days before the mandatory 30-day review period expired, John Peyton, a lawyer of the Agency's general counsel staff who served concurrently as the PRB's legal adviser, called and asked that I come to a meeting on March 26. He moaned audibly when I advised him that Mark Lynch of the ACLU would accompany me to the meeting. At the meeting, held in the general counsel's office on the seventh floor of the Headquarters building in Langley, the government's side was represented by five attorneys — three from the general counsel's office and two from the Justice Department. Had I come to the meeting alone, I would have been the lamb ready for slaughter. Because of his participation in other sensitive Agency cases, Lynch had earlier been granted a high-level "Q" clearance, but even so the Agency required him to sign an agreement before he could participate in that meeting. Peyton then explained that the publications review board had made 397 deletions in my manuscript. I was surprised, because I had been extremely careful not to use classified information in the manuscript. Those 397 deletions exceeded even the 339 passages excised from *The CIA and the Cult of Intelligence*, a book by John Marks and Victor Marchetti that deliberately set out to expose Agency secrets. I later learned that the 397 deletions represented only a fraction of those initially demanded by the Agency's Directorate for Operations. When I notified Peyton that I would be represented by the ACLU, the Agency had quickly retracted its more capricious deletions, resulting in the

final list of 397 items.

Lynch suggested that he and I first be permitted to adjourn to a private room to review each item. When we finished the review, the full group reconvened. I said that almost all deletions appeared in some form in the *Pentagon Papers*. Ernest Mayerfeld, deputy general counsel, said if that was true he could not object to their inclusion in the book. The lawyers said that I should get together the next day with the Agency's freedom of information officer, Bob, to consider specific deletions.

After lunch and later at home I reviewed the Agency's deletions and matched each item with my source documents. I was overjoyed: all significant deletions were covered by supporting public data. My joy was premature.

Early the next day I met Bob, who during my last few years with the Agency had served as my boss once removed. A dedicated cold warrior, Bob was a tall, stocky, impressive man in his late fifties who had achieved supergrade status in the Agency and had served as chief of station [19 words deleted].

Bob seemed as agitated as I, and it was obvious that he felt he was soiling himself by dealing with me. In less civilized circumstances we probably would have been happier fighting rather than talking. Early on Bob set the tone. "It's too bad you didn't work for the Israeli intelligence service," he said. "They know how to deal with people like you. They'd take you out and shoot you."

Bob then launched into a long monologue covering the vagaries of the secrecy laws, including details of the Carter administration's Official Disclosure Law, the Freedom of Information Act, and the various problems in their application. I impatiently endured this speech. I was most anxious to get on with the review, to produce my public documents, and to get the hell out of there.

We finally moved to the review of the specific deletions. The very first item caused trouble. Inexplicably the publications review board had deleted a reference indicating that the CIA conducted joint operations with Thai authorities. That relationship was so well known that books had been written about it, academic studies discussed it, pictures of CIA station chiefs appeared in the Thai press, and high-level Thai officials openly bragged in the media about CIA support for their organizations. Needless to say, I had not anticipated that the CIA would consider that relationship secret. If I could not admit that such a relationship existed, there was no point to the book since most of my observations were based on my six years with the Agency in Thailand. Fortunately I recalled a document from *The New York Times* edition of the *Pentagon Papers* entitled "The Lansdale Memorandum for Taylor on Unconventional Warfare," which discussed specific CIA operations conducted jointly with Thai organizations.

When I told Bob about the Lansdale memorandum being in the *Pentagon Papers*, he appeared to be surprised. But he recovered quickly and said there was only one official version of the papers — the Department of Defense's 12-volume edition. After numerous phone calls a secretary brought in 11 of the 12 volumes — the one missing volume, according to the index, was the one that most likely would include the Lansdale memo. This really shook Bob. He suspected that someone had removed the critical volume. Later we did get that volume, but the Lansdale memo was not in it. I argued that the Supreme Court's decision in the *Pentagon Papers* case had placed that information in the public domain, and it certainly could no longer be considered secret. We argued back and forth and finally agreed to postpone decisions on this and other items relating to CIA joint operations with Thai

LEADLY DECEITS

organizations.

Many deletions caused little problem. In some cases, where an ex-CIA official's affiliation with the Agency was well known, I had used that person's true name. The Agency objected. I felt the point was unimportant and agreed to substitute titles or aliases.

At one point I really became worried. Bob said that I must produce the document from which I had taken a direct quote. If I could not produce it, he warned that I would be accused of stealing secret documents. I had not deigned to steal any of the Agency's classified fantasy, but I was not sure that I could relocate that precise quote. Luck was with me that day, and a short scan of the research materials I had brought with me produced that quoted passage.

We referred the question of joint operations with the Thai police to the general counsel's office, which conceded that such information was probably not deletable. We continued our review based on the premise that I could discuss joint intelligence and counterinsurgency programs with the Thais. Even so, I could not mention my participation in programs with specifically named Thai organizations although I could substitute phrases to describe them. Also I was allowed, via footnoting, to replace a deleted item with information from a source document. By juxtaposition I hoped my meaning would be clear.

The next day I objected to the deletion of my very negative assessment of the Agency's long-term operations against mainland China. I produced a book, *Sub Rosa*, in which a former Hong Kong station chief, Peer de Silva, set forth his own lengthy, negative evaluation of those operations. I said Peer's book had been approved by the PRB and it had permitted him to state his opinion; therefore, I should be given the same privilege. Bob agreed and my critical comments, in modified version, were reinstated. From that point on I searched through books written by former Agency officials and cleared by the CIA, to locate items similar to deletions made in my book. By this tactic I was successful in reinstating numerous deletions.

We had a problem over naming specific CIA stations and bases — other than those already acknowledged — even though those installations were well known. The Agency's objection had nothing to do with secrecy. It instead applied to administering the Freedom of Information Act. Whenever the Agency acknowledged the existence of a station or base, the public could, under the act, demand documents relating to the facility. Although it seldom releases documents in response to such appeals, the Agency must by law physically check all such documents. By not allowing anyone to admit that a station or base exists, it avoids those requests.

Bob and I agreed to a modified version of my book. That weekend I made all the changes. On Monday morning I reviewed those changes with Mark Lynch and submitted the book to the deputy general counsel, Mayerfeld. In the interim Mayerfeld's office had reversed itself. He said *The New York Times' Pentagon Papers* had not been officially released, that the Supreme Court only ruled that it could not enjoin publication of those documents. Therefore, my discussion of liaison programs with Thai organizations might again encounter opposition.

That night I searched through the edition of the *Pentagon Papers* that Senator Mike Gravel of Alaska had entered in the official records of the Senate. I found that it included the Lansdale memorandum and therefore supposed that that constituted official disclosure. The next morning I happily relayed the news to Bob. He said members of Congress could say anything, so the Gravel edition did not count.

Official disclosure only occurs when a member of the executive branch of government performs that function. But how finely the Agency interpreted that statement I was yet to find out.

I immediately went to the Reston Regional Library to look for statements made by members of the executive branch relating to CIA operations with Thai organizations. I spent the day going through *The New York Times Index*, reviewing all entries under Thailand from the present back to 1954. The Index mentioned one well-publicized incident, allegedly caused by the CIA, that generated riots in Thailand. Because of the furor, numerous American officials were forced to comment on CIA operations in Thailand. Some press accounts sourced their information to CIA officials in Langley and the United States Embassy. I felt those references constituted executive branch disclosure of CIA activities in Thailand. I called Bob. He asked if the articles named specific American officials — a mere reference to a CIA official in Langley did not count. I said that Ambassador William Kinter had made a statement. He asked if the statement was in quotes. He said reporters could write anything, and if the statement was not in quotes it did not constitute official disclosure. (Later after completing the review process I found a reference to a high-level CIA official making a direct statement concerning CIA operations in Thailand.¹ I called Bob and asked if that did not constitute that ever-elusive official disclosure. He said no. That person had probably spoken unofficially and could be prosecuted for violating his secrecy agreement.) But as I continued to accumulate public evidence of the CIA's relationship with Thai organizations, Bob began to concede that I might retain relevant items in my book.

On Tuesday, April 8, I went to the Agency to rework the items deleted from my resubmitted version. I was not surprised to see that the Directorate for Operations had reversed itself in several key areas. Where its original deletions did not hold up, it merely changed its objections to apply to previously approved information.

China desk had changed its objection to my negative evaluation of its operations. The desk now claimed that the technique itself was classified. That technique, recruiting persons from the other side, was just slightly newer and less well known than prostitution. Of course if I could not discuss the technique, my evaluation would be meaningless. That night I went back to the Reston Library and cleaned out its shelf of books written by ex-Agency officials. Those books, some undoubtedly written at the behest of the CIA, discussed that "forbidden" technique in detail. By adding footnotes to those books, I was allowed to retain my discussion of that technique.

The Thai desk had also changed its position on material not initially marked for deletion — namely, the rural village survey program that I directed with Thai officials. The desk's original objection pertained only to my mention of working in liaison with Thais. When it became apparent it could not maintain that objection, the desk then claimed the technique itself was classified and must be deleted. This was ridiculous. Over the years I had lectured and passed out unclassified handouts describing the method. When documents reporting on those training sessions were located, the Thai desk had to drop its objection.

Forty-six days after I submitted the book, the Agency returned the manuscript with a letter saying that it had no security objections to the publication of that version. Throughout the review one central issue had been in question: reference to CIA operations with Thai organizations. What terrible secret was the CIA

200 DEADLY DECEITS

so vehemently attempting to hide? On October 6, 1976, Thai security forces overthrew the civilian, democratically elected government in a violent bloodbath. A study by Dr. E. Thadeus Flood published by the Indochina Resource Center said of that bloodbath: "This activist agency [CIA] took the lead in developing a strong apparatus in Thailand. . . . It should be mentioned that in their training, the CIA placed special stress on the Thai Border Patrol Police (BPP). News reports from Bangkok during and after the recent coup indicate that it was the Thai BPP who levelled their heavy weapons at unarmed Thai students, boys and girls, waving white flags, and raked them with fire."²

Thomas Lobe describes what happened in more detail: "On that horrible day in October 1976, then, the CIA/OPS-trained Border Patrol Police, with some units of the OPS-trained riot squads of the Metropolitan Police, burst into Thammasat University to crush the unarmed students and their fury knew no bounds . . . in meting out humiliations, in mutilizations brutally inflicted, in burning a student alive, and in simple wholesale murder. Thousands of unarmed students were killed, injured, or arrested, and a few days later, most of the liberal to left journalists, scholars, and intellectuals were also rounded up and put in prison or 'rehabilitation camps.'"³

After receiving the approved version of the manuscript, I signed a contract with a publisher who wanted extensive rewrites.

I began rewriting the manuscript and submitting each chapter as it was completed. On February 4, 1982, Paul Schilling, a young lawyer on the general counsel's staff, called and asked me to come to the Agency the next day for a meeting to discuss the first chapter. I was annoyed because everything in the chapter had either been approved before, was quoted from the Senate's Church Committee report, or was personal. I prepared myself with documents and met with Paul in one of the little anterooms off the main reception area. Some of the objections were to information that the Agency had declassified and released to the Church Committee, which I easily documented. But the other objections concerned details of my training in espionage and paramilitary operations and details of psychological tests the Agency uses to help identify a specific personality type for possible employment. I was not prepared to rebut those arguments. Paul and I agreed that I would return home and call in the appropriate references.

The rest of the day I phoned around to all Fairfax County libraries to get copies of books by William Colby, Ray Cline, Allen Dulles, Lyman Kirkpatrick, David Phillips, and other pro-Agency authors whose works had received formal CIA approval if not sponsorship. Almost all discussed information that the PRB now claimed was classified. I phoned the citations in to Paul Schilling. I thought that would take care of the matter. A few days later Paul called and asked if I would come in for another meeting. On February 11 we met again in one of the cubbyholes off the packed main reception area. Paul apologized for asking me in again and said that the PRB had agreed that the information I had taken from the Church Committee report was not classified. I relaxed. The PRB was merely recognizing reality.

Paul then said, "But the other material on your training and the psychological test is classified. The board said it had made a mistake earlier when it had approved that information."

To the shock of the people in the reception area I bellowed, "That's tough shit. It can't reclassify information." After calming down, I pointed out that the

Agency had cleared similar information on training for its friendly former officers such as Colby, Phillips, Cline, Dulles, Kirkpatrick, and others.

"Yes," Paul said, "but the PRB made mistakes."

I noted that in at least one case the CIA had helped a former officer write his book, and the book contained numerous references to training.

Paul responded, "The Agency's relationship with an author is that the PRB reviews material written by the author, nothing else."

"That's not the case with [the book in question]. It was written as a c action project by the Agency. I know it was."

Paul continued, "The Agency's relationship with an author. . . ."

I then cited facts relating to the writing of that book.

Paul retorted, "The Agency's relationship with an author. . . ."

Schilling recommended that I consider an appeal to the deputy director of the CIA, Admiral Bobby Inman.

That weekend I called Paul at home and advised him that Executive Order 12065 on classification, Section 1-607, reads: "Classification may not be restored to a document already declassified and released to the public under this order or prior orders." Paul said, "Oh, we're operating under a new order." What Paul was referring to was a draft executive order then being proposed by the Reagan Administration. That order, only later put into effect, allows officials to reclassify information previously declassified and disclosed if it is determined in writing "that the information requires protection in the interest of national security and if the information may be reasonably recovered." The manuscript obviously could not be "reasonably recovered," since I had sent copies to my publisher, my editor, and numerous others.

Paul quickly realized he had jumped the gun on the new executive order and shifted instead to the position that Agency officials had again and again made mistakes in declassifying information in my original manuscript and in other books.

After consultation with Mark Lynch, I prepared and submitted my 35-page appeal on February 19, 1982, noting that many of the deleted items had been approved in the first manuscript, had appeared in the approved writings of other pro-Agency officers, or were available in numerous other publications. On March 12, 1982, I received a letter from the general counsel's office saying, "The DDCI [deputy director of central intelligence] has reversed the board with respect to all . . . passages contested in the appeal," except that, "the DDCI has upheld the board's decision to delete five sentences . . . unless Mr. McGehee can show the Agency has previously cleared such information."

I immediately scanned four approved books and found 24 references to equivalent or identical material as contained in the five sentences. I sent these references to the general counsel. The PRB acted quickly and, rather embarrassed, acknowledged that my five sentences were not classified.

I thought, well, now I have been vindicated and my problems are over. But this was not to be. On March 23, I received another letter informing me that chapter two was so sensitive that it was impossible to identify specific items and the PRB had rejected the entire chapter. I had had enough and contacted George Lardner, Jr., a journalist with *The Washington Post*. He wrote a long article entitled "CIA Veteran Decries Effort to Reclassify Material for His Book." This public embarrassment forced the Agency to reconsider its actions. On April 29, I received a registered letter offering me the services of Bob — my old antagonist — to work

202 DEADLY DECEITS

together to produce an approved version of the manuscript.

I accepted the offer. We held three long sessions at my office, so we would have instant access to my books and files. The battle over chapter one had been completed, so we concentrated on the remaining chapters that I had turned over in the preceding months. Chapter two, dealing with my tours in Japan and the Philippines, according to the earlier PRB decision could not be used, but in the interim I had stumbled upon one of the lesser-known books by ex-CIA officials, Howard Hunt's *Undercover*. In it, to my joy, was a chapter dealing with his assignment as a case officer to Japan; the same chapter also discussed the Agency's base at Subic Bay in the Philippines. His book had been approved by the Agency and when I pointed this out to Bob he agreed that I should also be permitted to discuss my activities in those countries. Even so, I was not allowed to include details of my work. I could only give information no more explicit than that given in *Undercover*.

Chapter three also presented major problems. Many of my specific designations for places were deemed classified, but by making minor changes I was allowed to retain some points. The discussions of my work at Headquarters processing clearances and file traces were marked classified and many sentences had to be deleted. Although the Marchetti-Marks and Colby books had discussed the requirements for clearances and traces, they had not gone into any detail. Unable to locate other coverage of these procedures, I could not retain my material. But I was allowed to quote information on that topic given in Philip Agee's book, *Inside the Company*.

Chapter four, about my tour on Taiwan, gave information in general terms of an agent operation directed at mainland China. Someone had objected to this major element of the chapter. I protested that other approved Agency authors had been allowed to discuss agent operations, some with a great deal more specificity than my account. This argument was finally accepted.

Bob and I reviewed each of the many points in the remaining chapters. In this process I conceded a number of points where the law was clearly on my side. I did this to speed the clearance process and to avoid a long, time-consuming lawsuit.

John Marks and Victor Marchetti's book *The CIA and the Cult of Intelligence*, published in 1974, was the last approved critical book written about the Agency by an ex-employee. In light of my own experiences the reason is obvious: the secrecy agreement and the way it is abused by the Agency. It is virtually impossible to write in an atmosphere where everything is secret until it is deemed otherwise. The PRB, taking its responsibilities seriously, labels just about everything secret until an author who is critical of the Agency can prove this not to be the case. But the situation for ex-employees who are advocates of the CIA is the opposite. They are given almost *carte blanche* to discuss operations and techniques, and in some instances they are assisted in the research and writing of their works.

Does the secrecy agreement work to protect legitimate classified information? Probably to some small degree it does. But the price we pay for this minor protection is enormous. The Vietnam War is a prime example. This Agency-produced disaster was sold to the American people through massive disinformation operations. Would it not have been better if we had known the truth at an early stage? Similarly, would the American people not be better off knowing the truth

about the CIA's current secret war in Latin America? Don't we deserve to know about reckless and phony covert operations, including Agency-planted "Communist" documents, that help determine our foreign policy?

It is clear that the secrecy agreement does not halt the flow of information to our enemies, for it does not affect the CIA employee who sells information. Look, for example, at England, which has a strict official secrets act and probably the most porous security service in the western world. What the CIA's secrecy agreement does quite effectively, however, is to stop critics of the Agency from explaining to the American public what the CIA is and does. It is sad to say, but the truth is that the primary purpose of the secrecy agreement is to suppress information that the American people are legitimately entitled to. For this reason, I am opposed to the secrecy agreement as it is now written and administered.

Because the major portion of my CIA career revolved around Southeast Asia, where CIA operations were well publicized and even officially disclosed, the Agency could not stop release of much of the information in this book. But my experience should sound a warning. Agency officials show no hesitation in trying to censor embarrassing, critical, or merely annoying information. I cannot speak for the legal aspects of the various laws, but it is obvious that national security has little to do with how the Agency administers the secrecy agreement. As the CIA becomes more adept at applying the law under President Reagan's executive order on classification that went into effect August 1, 1982, all critical information about the Agency will probably be forbidden.

I do not expect that the executive branch or the Supreme Court will be upset by the Agency's attempts to censor information that the public is entitled to. The American people, however, should be worried. Once the Agency is unleashed and the iron curtain of official disclosure falls, we will all suffer its consequences.

APPENDIX 2

APPENDICES TO HEARINGS HELD NOVEMBER 3, 1983

APPENDIX I.—MISCELLANEOUS MATERIALS

- Letter from Professor George I. Davida, University of Wisconsin—Milwaukee, to Hon. Robert W. Kastenmeier dated October 28, 1983. Attachment: "American Council on Education, Report of the Public Cryptography Study Group," February 7, 1981.
- Letter from Jonathan Knight, Associate Secretary, American Association of University Professors, to David Beier, Esq., Counsel, House Committee on the Judiciary, dated October 31, 1983. Attachment: "American Association of University Professors, Government Censorship and Academic Freedom."
- "American Association for the Advancement of Science, Project on Secrecy and Openness in Scientific and Technical Communication," October 1983.
- Letter from William D. Carey, Executive Officer, American Association for the Advancement of Science, to Hon. Robert Kastenmeier, dated February 15, 1984.
- Letter from A. Bartlett Giamatti, President, Yale University, to Hon. Robert Kastenmeier, dated December 12, 1983.

APPENDIX II.—ARTICLES AND PAPERS

- "American Civil Liberties Union, Free Speech, 1984: The Rise of Government Controls on Information, Debate and Association," July 1983.
- Relyea, "Shrouding the Endless Frontier—Scientific Communications and National Security: Considerations for a Policy Balance Sheet," 1 Gov't Information Q. 1 (1984).
- Gelbspan, "U.S. Tightening Access to Information" (3-part series), Boston Globe, January 22, 23, 24, 1984.
- Ehlke & Relyea, "The Reagan Administration Order on Security Classification: A Critical Assessment," 30 Fed. Bar News & J. 91 (1983).
- "American Association for the Advancement of Science, Scientific Freedom and National Security," June 1984.
- "Federal Restrictions on Research: Academic Freedom and National Security," Academe, September/October 1982 at 19.
- Gray, "Technology Transfer at Issue: The Academic Viewpoint", IEEE Spectrum, May 1982, at 64.
- Wallich, "Technology Transfer at Issue: The Industry Viewpoint," IEEE Spectrum, May 1982, at 69.
- Pyle, The Invasion of Privacy, 34 Proc. of the Acad. of Pol. Sci. 131 (1982).
- Kamen, "Appeals Court Upholds CIA Censorship of Article," Washington Post, October 5, 1983.
- "National Security and Scientific Freedom," AAAS Committee on Scientific Freedom and Responsibility Bulletin, September 1982.
- Massachusetts Institute of Technology, Interim Report of the Committee on the Changing Nature of Information, March 9, 1983.
- Unger, "The Growing Threat of Government Secrecy," Technology Review, February/March 1982 at 31.
- R. Park, Scientific Freedom: Where Does Congress Stand? (unpublished paper).
- Chalk, "Commentary on the NAS Report," 8 Science, Technology, & Human Values 21 (1983).
- Rosenbaum, Tenzer, Unger, Van Alstyne & Knight, "Academic Freedom and the Classified Information System," 219 Science 257 (1983).
- American Association for the Advancement of Science, Committee on Scientific Freedom and Responsibility, National Security and Scientific Communication (June 1982).
- W.D. Cooke, T. Eisner, T. Everhart, F. Long, D. Nelkin, B. Windom, E. Wolf, Restrictions on Academic Research and the National Interest (unpublished paper).
- Ferguson, "Scientific Freedom, National Security, and the First Amendment," 221 Science 620 (1983).
- Ferguson, "Scientific and Technological Expression: A Problem in First Amendment Theory," 16 Harv. C.R.-C.L. L. Rev. 519 (1981).
- Corson, "What Price Security?," Physics Today, February 1983, at 42.
- Pike, "When Science is Outlawed," Inquiry, March 29, 1982, at 21.
- Harvard University, Federal Restrictions on the Free Flow of Academic Information and Ideas, January 1985.



THE UNIVERSITY OF WISCONSIN—MILWAUKEE/P.O. Box 784, Milwaukee, Wisconsin 53201

COLLEGE OF ENGINEERING AND APPLIED SCIENCE
DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
(414) 963-4677

October 28, 1983

The Honorable Robert W. Kastenmeier
The House of Representatives
2232 Rayburn House Office Bldg.
Washington, DC 20515

Dear Congressman Kastenmeier:

This is in response to your inquiry regarding my experience with the government's classification power.

In 1977 the Wisconsin Alumni Research Foundation filed for a patent on behalf of myself and a graduate student for a data protection device that resulted from research funded by the National Science Foundation. The research was unclassified and was based on materials publically available. In 1978 we were issued a secrecy order by the Commerce Department which, unknown to us at the time, had done so at the request of the National Security Agency.

Upon careful reading of the secrecy order, we became concerned since the order contained penalties of two years in jail and \$10,000 fine for unauthorized disclosure of the subject matter of the patent application, which, I would like to emphasize, was based on publically available material.

Upon informing the University of the secrecy order, the Chancellor became quite concerned that the order infringed on academic freedom, not to mention the First Amendment. After the resulting press coverage, the Chancellor communicated with the then Commerce Secretary Krepps and NSA director Admiral Bobby Inman. A short time later, the order was rescinded.

In 1979 the Americal Council on Education undertook a study of the issue of publication of research in Cryptography and its relation to national security. The group, called the Public Cryptography Study Group (PCSG), met for about two years and in 1981 issued a report in which the majority of the members recommended a system of "voluntary" prior review. I dissented from this recommendation and issued a minority report in which I outlined my reasons for opposing what I saw as nothing more than censorship.

The People of Wisconsin's Urban Engineering College
Serving Milwaukee, the State and the Nation

My opinion has not changed. I still oppose the system of prior review. My concern has grown as I have seen my predictions, that the government's interest in classification of research would grow to include other areas, come true.

The secrecy orders and the PCSCG's recommendations raised issues that had a direct bearing on the Nation's political, scientific and economic health. More specifically, the secrecy orders and prior review raised questions regarding:

1. Constitutionality

The secrecy order that was issued to us was for material that we had discovered without knowledge of classified information. The government seemed to regard this subject to be what some have called "born secret." Such concepts have no place in our democracy.

2. Impact on Basic and Applied Research

Secrecy orders and censorship of results deemed by some in the government to be a danger to the national security would inevitably lead to the removal from the public domain of interesting results. There is no doubt that this would seriously harm the quality and direction of research.

The PCSCG's recommendations were equally disturbing. It was without any basis since the committee had no evidence to suggest that publications in cryptography were harmful to the nation's security. The committee did not consider the critical importance of cryptography in data protection. Our nation is changing. The most intimate details of our lives are being stored and manipulated by computers. Medical databases, credit files, insurance files, employment records are being constructed and connected to computer networks. These technological changes can potentially destroy not just privacy, which is already gravely threatened, but freedom itself. It is difficult to conceive of freedom without privacy.

Economically, our society is changing in such a way that our assets are no longer physical, but logical. Disks and not vaults are the repository for the new wealth. Wealth is being reduced to just "bits" and "bytes" in some computer. Electronic funds transfer would make it possible to move this wealth at unprecedented speeds.

The need for protection technology was made abundantly clear in the reported Soviet evesdropping activities. More recently young computer buffs raided computer systems all over the country. What caused these weaknesses? In the case of

cryptography, the government would not only not share its knowledge in data protection, but was now attempting to suppress information developed in the civilian sector. These actions clearly indicate that the blame for the vulnerabilities in our communication and computer rests with the government.

3. Effectiveness of Such Measures

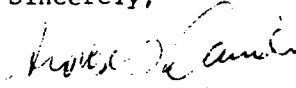
Even if one was willing to ignore all the other objections to suppression of information, there still remained the question of whether the actions would have the desired effect of denying the results to our enemies. There is no evidence that there is significant contribution to technology transfer to our enemies by publications of basic research. Studies have shown that technology transfer to our adversaries occurs through commercial exports from both the United States, Western Europe and Japan. What little impact from publications there may be has to be balanced against the obvious benefits that this nation enjoys in just about every area of technology that we choose to pursue. We are clearly the world leaders in those areas that we are equipped to conduct research in. There are areas in which, some say, we are losing our lead to, not the Soviets, but the Japanese. The decline of investment in research has been well documented. It, therefore, should not surprise anyone if we lose our lead in areas that are underfunded. Our shortcomings are not due to lack of ability. Our problems have been the lack of national leadership to reinstate the resources necessary to maintain (or regain) our technological lead.

In assessing our technological strengths and weaknesses, some comparisons are in order. Just how well are we doing compared to, say, the Soviets? It is interesting to note that in the non-defense R&D and production, we are clearly decades ahead of the Soviet Union. But when we consider nuclear weapons, government officials at the highest levels tell us that the Soviets are either equal to us (the prevailing view) or are slightly ahead. It thus appears that in an area where both we and the Soviets practice secrecy, the results are about the same! This is rather strange since one would expect that, in a field where we were practicing secrecy and thus denying the Soviets the opportunity to share in our advances, we would be ahead given our overall lead in technology. This implies that if we were to impose secrecy in other areas of engineering and science then what we can expect is that we will do about as well as the Soviets. Secrecy, it seems, has only thing one in store for us: mediocrity.

It is also possible that if efforts to restrict the flow of information continue, then not only will they damage our research capability, but may very well start an "information war" with our friends.

Finally I, like many others, am concerned about the inconsistency of my government's actions. The government sells the Russians wheat to help feed them and then turns around and tells us that we must not communicate among ourselves lest we help the Russians. Apparently the government believes that it can better protect us from the Russians if it keeps the Russian stomachs full and our minds empty.

Sincerely,

A handwritten signature in cursive script, appearing to read "George I. Davida".

George I. Davida
Professor

cc

REPORT OF THE PUBLIC CRYPTOGRAPHY STUDY GROUP

Prepared for

American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

FOREWORD

This report has been prepared by the members of the Public Cryptography Study Group.¹ The Study Group was assembled by the American Council on Education (ACE) in response to a request by the National Security Agency; that agency has indicated concern that information contained in some articles in learned and professional journals and in monographs might be inimical to the national security. The Study Group held its first meeting on March 31, 1980, and transacted its business in a series of meetings through February 1981. (The membership of the Study Group is listed on page 2.)

The Study Group has recommended that a voluntary system of prior review of cryptology manuscripts be instituted on an experimental basis. While the group would prefer no such system of review, its members, with one dissent, accepted as a working premise NSA's concern that some information contained in cryptology manuscripts could be inimical to the national security of the United States and see the proposed system as a potential way to test that working premise. The group rejected a compulsory statutory solution to the perceived problem.

In assembling the Study Group, ACE sought recommendations of individuals who might participate from several professional societies and organizations. The American Association of University Professors (AAUP), the American Mathematical Society (AMS), the Association for Computing Machinery (ACM), the Computer Society of the IEEE (IEEE/CS), the Institute of Electrical and Electronics Engineers (IEEE), and the Society for Industrial and Applied Mathematics (SIAM) made such recommendations. Although nominated by professional societies, the members served as individuals on behalf of ACE and the final report is a product of the American Council on Education.

The Study Group hopes that the recommended voluntary system will prove effective. Success, however, is dependent upon the endorsement and good faith cooperation of NSA on one side and authors, researchers, professional societies, and publishers on the other. Therefore, it is the intent of the Study Group that this report be transmitted to all relevant professional societies, as well as receiving widespread public distribution. The Study Group also recommends that a timely review be conducted concerning the operations of the recommended voluntary system, should one emerge, and that the relevant professional societies receive and record comments on such operations for use in the future review.

¹This material is based upon work supported by the National Science Foundation under Grant No. CDP-8006675. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the National Science Foundation.

MEMBERSHIP

Dean Werner A. Baum — CO-CHAIRMAN
College of Arts and Sciences
(and Chancellor Emeritus, U. of Wisconsin - Milwaukee)
The Florida State University
Tallahassee, FL 32306

David H. Brandin
Vice President
Computer Science and Technology Division
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025
(Nominated by the Association for Computing Machinery)

Professor R. Creighton Buck
Department of Mathematics
Van Vleck Hall
University of Wisconsin
Madison, WI 53706
(Nominated by the American Mathematical Society)

Professor George I. Davida
Department of Electrical Engineering and Computer Science
University of Wisconsin - Milwaukee
Milwaukee, WI 53201
(Nominated by the Computer Society of IEEE)

Professor George Handelman
Department of Mathematical Sciences
Rensselaer Polytechnic Institute
Troy, NY 12181
(Nominated by the Society for Industrial and Applied Mathematics)

Professor Martin E. Hellman
Department of Electrical Engineering
Stanford University, Durand 135
Stanford, CA 94305
(Nominated by the Institute of Electrical and Electronics Engineers)

Chancellor Ira Michael Heyman — CO-CHAIRMAN
Chancellor's Office, 200 California Hall
University of California, Berkeley
Berkeley, CA 94720

Professor Wilfred Kaplan
Department of Mathematics
The University of Michigan
347 West Engineering Building
Ann Arbor, MI 48109
(Nominated by the American Association of University Professors)

Daniel C. Schwartz
General Counsel
National Security Agency
Central Security Service
Fort George G. Meade, MD 20755

I. INTRODUCTION

Two years ago, Vice-Admiral B. R. Inman, Director of the National Security Agency, publicly indicated his deep concern that some information contained in published articles and monographs on cryptography² endangered the mission of NSA and thus the national security. Existing statutes do not regulate the domestic publication of unclassified information relating to cryptography.³ Admiral Inman proposed a dialogue with the academic community on how to reconcile the national needs with the tradition that scholarly publication should be free from restriction.

In response to Admiral Inman's initiative, the American Council on Education proposed establishment of a Public Cryptography Study Group, bringing together representatives of the academic world and of NSA. The National Science Foundation agreed to provide funding to the ACE for this purpose. This report is the product of the Group's efforts over a year.

In addition to the dilemma of reconciling important First Amendment rights with NSA's concern for the protection of the nation's communications security and intelligence-gathering capabilities, the group soon recognized that it was essential to take into account the emerging uses of cryptography in the public sector.

In an era of instantaneous communication and pervasive computer data bases, it is becoming increasingly important to protect the privacy of both individuals and corporations, often using the tools previously used only by national governments.

There is growing evidence that enhanced security for unclassified but sensitive information will be needed in a wide variety of applications, ranging from personal records (insurance, criminal, health, law enforcement) to commercial proprietary and financial data in storage or in

²Cryptography is the body of knowledge that deals with methods of information protection. Methods that transform text, using a key, so that it becomes unintelligible and therefore useless to those not meant to have access to it, are called *encryption* methods. Transforming the encrypted information back to its original form is called *decryption*.

³Provisions of the United States Criminal Code and related regulations make it a crime to receive, disclose, communicate, or publish various kinds of documents and information. Section 798 of Title 18 specifically prohibits knowing communication, transmission, or publication of any *classified* information pertaining to any "code, cipher or cryptographic system," or any "communication intelligence activity" of the United States or any foreign government to an unauthorized person. It also prohibits the use of such classified information in a manner prejudicial to the interests of the United States or to the benefit of any foreign government. Section 793 of Title 18 prohibits the obtaining or delivering of information relating to the national defense with knowledge that the information is to be used or could be used to the injury of the United States or the advantage of any foreign nation, or revealing national defense information through gross negligence where the information was initially in the individual's lawful possession. In addition, 18 U.S.C. Section 952 prohibits dissemination of information about diplomatic codes. A related statute, 50 U.S.C. Section 403(d), charges the Director of Central Intelligence with the responsibility to protect intelligence sources and methods pursuant to which he has promulgated intelligence directives binding only on the government.

transit electronically. As the major world economies continue the trend toward information dependence, e.g., electronic mail, electronic funds transfer, point of sale terminals, etc., protection of business and even home computer systems from unauthorized monitoring or tampering will become increasingly important.

In many of these areas, cryptography is one of the most effective ways for providing the requisite security. Restriction of public research and development in cryptography might have an adverse effect on the ability of American industry to compete in world telecommunications and data-processing markets.

2. THE NATIONAL SECURITY CONCERNS

Traditionally, national security information has been of a diplomatic or military nature. However, as the nation moves to an information-based economy, protecting valuable or sensitive commercial and personal information becomes a concern of national security in a broader sense. Inadequate security for such data could have profound effects on the nation.

The Study Group recognizes that increased research activity in cryptology by persons and institutions in the nongovernmental arena may result in advances in the development of cryptographic systems. Work directly in cryptology or in related fields may have a beneficial impact on developments in computer science, electrical engineering, and mathematics which have potential benefits to fields apart from cryptology. Products developed in the course of this research may be very useful in providing effective telecommunications for nongovernmental and governmental purposes. Although governmental efforts in cryptology have traditionally led private efforts, these private efforts may develop new techniques or insights that could benefit broader government interests. The Study Group also recognizes that significant nongovernmental research in this area may be applied over the long run to increase communication protection in commercial and private fields, thus enhancing the security of private and commercial communications and ultimately furthering the nation's welfare and security in a broader sense.

Some researchers in the public sector have expressed serious concern about the fragility of our developing information-based society. It has been suggested, for example, that a foreign power might inject misleading data into the statistics used for computing the nation's money supply, causing the government to take dangerously inappropriate action.

At the same time, however, concerns have been expressed by the National Security Agency that extensive private work in cryptology and related fields may significantly and directly adversely affect the security of the nation's sensitive official communications and the nation's ability to obtain and understand foreign intelligence. NSA claims that the risks become greater to the extent that work moves away from pure research and into the application of theoretical developments to specific problems of communication protection and the development of actual protection systems.

One of the areas of concern by the NSA is that substantial work in cryptographic and cryptanalytic techniques together with a widespread dissemination of resulting discoveries could lead to the publication of cryptographic principles or applications similar to those used by the United States Government. NSA claims that this work may enable foreign powers to engage more successfully in cryptanalytic attacks upon the secure telecommunications of our government. Another area of concern to the NSA is that papers dealing with weaknesses in

cryptosystems that may be used by other governments may alert these governments to the weaknesses of their own systems and thus prompt them to adopt more sophisticated and less vulnerable systems. In this manner, the United States may be denied needed intelligence.

The National Security Agency has expressed interest in considering what type of procedure could be developed that would provide a systematic means by which publications relating to cryptology could be reviewed to determine whether such publications would have an overriding adverse impact on the national security as it pertains to NSA's mission. There exist a number of federal statutes and regulations that govern the dissemination of information that is classified or controlled by the U.S. Government on the basis of national security or foreign policy concerns. It is felt by NSA, however, that these statutes and regulations do not cover publication of articles or the dissemination of general research information within the United States. They also may not cover such publication abroad unless such information is otherwise classified by the government or its export is controlled for national defense or foreign policy reasons.

Existing statutes do not regulate the domestic publication of unclassified information relating to cryptology. Restrictions on foreign dissemination of certain information relating to cryptology are contained in the provisions of the Arms Export Control Act (22 U.S.C. 2778), which authorizes the President to compile a United States Munitions List and to issue the International Traffic and Arms Regulation (ITAR) (22 CFR 21), which identifies specific types of articles, the export of which is subject to the granting of a license by the Secretary of State. Cryptographic equipment is explicitly designated as a category subject to such export control. Category XVIII of the ITAR includes technical information relating to articles on the Munitions List. This latter provision has been subject to some question by the Office of Legal Counsel in the Department of Justice as being overly broad.

Munitions Control Letter No. 80, February 1980, issued by the Department of State provided further clarification under ITAR with respect to cryptology by making clear that the export restrictions do not prescribe prepublication review for publication in the United States of any publications including "general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment" otherwise covered by the export licensing restrictions.

There has been some disagreement within the government concerning the extent of the need to control technical data. The Department of Commerce, in the context of a review of the Export Administration Act, has indicated that its assessment is that the availability of technical data that are of significance to U.S. national security and foreign policy interests is likely to be minor. On the other hand, the Departments of Defense and State, in the context of the Arms Export Control Act under which the ITAR is promulgated, have continued to emphasize the need to effectively control technical data. In addition, studies conducted for the Department of Defense led to the establishment within the Export Administration Act of the

Military Critical Technologies List, which is heavily focused on knowledge related to design, manufacturing, application, operation, and maintenance of such critical technologies. Cryptographic items are not processed under the Export Administration Act of 1979 unless there is a prior determination by the Department of State that jurisdiction over a specific item should be transferred to Commerce for processing under that Act.

Finally, Section 181 of Title 35 U.S.C. permits the imposition of a secrecy order upon a patent application when issuance of a public patent would be detrimental to the national security. The statute also provides for compensation for the nongovernment inventor financially injured as a result of a secrecy order. There is no provision in the law pertaining to patent secrecy orders that applies directly to publication or to any requirement for prepublication review. Additionally, a patent secrecy order for a patent application based on published material is not possible.

While there is currently no formal procedure or requirement for prepublication review by NSA of publications relating to cryptology, some authors and publishers routinely and voluntarily submit proposed publications to NSA for review and comment as to the sensitivity of the information involved. NSA currently has no statutory authority to require submission of proposed publications for the purpose of review or to require changes in publications prepared outside the agency and not under NSA contract or grant. The National Science Foundation has announced, however, that, while it does not currently have classification authority, it has responsibility under routine executive orders to refer information developed in NSF-supported cryptologic research it believes may be classifiable to NSA for possible classification.⁴ NSF indicates, however, that it makes no essential difference, from the standpoint of classification, whether research is supported by NSA or NSF.

⁴The following text, included for completeness, is the standard NSF Grant Instrument Clause for Potentially Classifiable Research.

The National Science Foundation does not expect that results of basic research it supports will be classified, except in very rare instances. Further, while NSF does not have classification authority, it has the responsibility to refer any information that NSF has reason to believe might require classification to the agency with appropriate subject matter interest and original classification authority.

Therefore, the grantee is responsible for immediately notifying the NSF Program Official, of any data, information, or materials developed under this grant which may require classification. The grantee shall, prior to dissemination or publication of potentially classifiable research results obtained under this grant, allow NSF the option to review such materials. The grantee shall defer dissemination or publication pending the review and determination that the results are not classified, provided such review and determination are completed within sixty days of receipt by NSF of such material. If the review results in classification, the grantee agrees to cooperate with NSF or other U.S. agencies in securing all related notes and papers. Policies relating to this subject are set forth in the NSF *Grants Policy Manual* Section 794, "National Security."

3. DELIBERATIONS AND CONCLUSIONS

As a starting point for its work, Admiral Inman proposed that the Study Group consider the acceptability of restrictions on domestic dissemination of nongovernmental technical information relating to cryptology. He proposed several criteria that should be taken into account for both policy and legal reasons:

- (1) The restrictions should apply only to a central core of critical cryptologic information that is likely to have a discernible adverse impact on the national security.
- (2) Law and regulations should make these criteria as clear as is possible without revealing information damaging to the national security.
- (3) The burden of proof in imposing any restriction on dissemination should be borne by the government.
- (4) There should be judicial review of any such government action, perhaps by a specially constituted court that could act under suitable security precautions, and the government should bear the burden of obtaining judicial approval of its action.
- (5) There should be full, fair, and prompt compensation for any company or person losing the economic benefit of information by virtue of governmentally imposed restrictions on dissemination.

Admiral Inman's criteria would suggest a statute that would create a system of restrictions. There are basically two ways to proceed by statute. One is to make it a crime to disseminate defined cryptologic information. Under such a system, NSA (or another agency) would monitor published information and would recommend criminal prosecution in instances where defined cryptologic information had been published. The other means is by required prepublication review. The statute would make it mandatory to obtain clearance from a designated agency, such as NSA, before publishing defined cryptologic information. Publishing without obtaining clearance would be a criminal act. The impact of the latter system could be moderated, as suggested by Admiral Inman, by requiring a judicial order confirming the agency's decision to restrict dissemination and by payment of compensation where permission is denied. Still, however, it would be a crime to publish without seeking clearance or in contempt of the judicial restraining order.

Admiral Inman's criteria suggest a system of prepublication review. Such a system clearly would best serve Admiral Inman's concern by assuring the government's ability to preclude publication or dissemination of defined information. At the same time, however, such a system raises serious legal, policy, and practical questions.

Problems Associated with a Nonvoluntary System

The legal and political system of the United States, as expressed in the First Amendment to the Constitution, is generally opposed to both pre- and postpublication restraints. Although such opposition, historically, has been strongest where restraints have been placed on utterances related to political or social thought, the First Amendment applies to practically all speech, regardless of its description, with the possible exception of obscenity.⁵ (For instance, the present Supreme Court has applied First Amendment protections to "commercial" speech, which previously had been treated as outside the ambit of the First Amendment.⁶ Further, courts, as in the recent *Progressive Case*,⁷ have assumed without debate that information of a technological or scientific nature is subject to First Amendment protections. It is clear that monographs and articles in professional journals and elsewhere concerning cryptography are within the ambit of this protection. As one legal scholar has observed, freedom of expression has historically related to four traditional and interrelated values:⁸

- (1) individual self-fulfillment,
- (2) the advance of knowledge and the discovery of truth,
- (3) participation in decision making by all members of society, and
- (4) maintenance of the proper balance between stability and change.

Writings on cryptology are closely related to (1) and (2), if not also to (3) and (4).

That speech falls within the protection of the First Amendment, however, does not mean that it cannot be regulated. In most recent instances, the Supreme Court has sought to balance the importance of the speech involved against the state interest sought to be protected by its regulation. In many cases, the Court has weighted the balance heavily in favor of free speech (a "preferred freedom") and subjected the opposing interests to "exacting scrutiny."⁹ In others, it has been neutral or has weighted the balancing to the contrary.¹⁰ It is difficult to discern a consistent theory with predictable results.

⁵*Roth v. United States* 354 U.S. 476, 1957. Even though determined to be outside the bounds of the First Amendment, because it is so removed from the "advancement of truth, science, morality, and arts in general... and its lack of redeeming social importance," the Court has carefully and consistently delineated narrow standards for permissible restraints on obscenity. Four dissenters to obscenity controls (Brennan, Stewart, Marshall and Stevens) are of the view that any such controls, at least for adults, are unconstitutional.

⁶*Bigelow v. Virginia*, 421 U.S. 809 (1975). See Emerson, *First Amendment Doctrine and the Burger Court*, 68 CAL. L. REV. 422, 458-61 (1980) (hereafter "Emerson").

⁷*United States v. Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis.), request for writ of mandamus, den. sub. nom. Morland v. Sprecher, 99 S. Ct. 3086, case dismissed, Nos. 79-1428, 79-1664 (7th Cir. Oct. 1, 1979).

⁸Emerson 423

⁹Emerson 449

¹⁰Emerson 450-51

It is likely that the Court would balance in a neutral manner where the justification, adequately demonstrated, was that publication constituted a threat to national security.¹¹ The government, of course, would bear the initial burden of showing that such publication posed a significant threat.¹² Once this was shown to the Court's satisfaction, the issue properly would be whether the threat to security by the publication of a writing concerning cryptology outweighed the value of the writing itself, the maintenance of nongovernmental research programs in cryptology, unfettered academic and scientific inquiry, and similar threatened social values. Such a test, of course, could not come about without passage of legislation barring publication of privately generated information concerning cryptology. The legislative balancing implicit in its passage undoubtedly would be given some weight by the Court. Of considerable importance would be whether or not the legislation narrowly defined the regulated information. The legislation would more easily pass judicial scrutiny if a narrow and unambiguous definition was formulated because its chilling impact on cryptologic research would be minimized.

Historically, the *means* of regulating expression has been of central importance to constitutional validity. Although some regulation or restraint may be justified, the Court usually has required that the least drastic means be used. Punishment for uttering or otherwise publishing proscribed speech has been difficult to maintain; imposing a licensing system — or prior restraint — has been much more difficult. "The doctrine forbidding prior restraint is one of the major underpinnings of the system of freedom of expression. Its roots go back to the English censorship laws against which John Milton protested."¹³

There have been exceptions, however, to prohibitions on systems of prior restraint. One seminal case stated that the publication of "the number and location of troops" could be restrained.¹⁴ The trial court in the *Progressive Case*¹⁵ enjoined the publication of materials concerning the design and operations of nuclear weapons. The Supreme Court in another case¹⁶ permitted a censorship board to screen out "obscene" films. Moreover, the present Supreme Court "does not [appear to] view the prior restraint doctrine as a prohibition on all prior restraints subject to certain categorical exceptions such as obscene motion pictures or communications about tactical military operations. Rather, in its view, the doctrine simply creates a

¹¹Goldberg, *The Constitutional Status of American Science*, 1979 UNIV. OF ILL. L. FORUM 1, 14-15 (1979)

¹²*New York Times Co. v. United States*, 403 U.S. 713 (1971)

¹³Emerson 454

¹⁴*Near v. Minnesota ex rel Olson*, 283 U.S. 697 (1931)

¹⁵Note 7, *supra*.

¹⁶*Times Film Corp. v. City of Chicago*, 305 U.S. 43 (1961)

'presumption' against the validity of the restraint and thereby imposes a 'heavy burden' on the government to justify the particular restriction then before the Court."¹⁷ This is buttressed by the Court's action in the *Pentagon Papers Case*.¹⁸ Three justices (Burger, Harlan, and Blackmun) would have upheld the injunction, believing that the courts should exercise only an extremely limited review where the executive has determined that the disclosure "would irreparably impair the national security." Thus they did not even require the satisfaction of a "heavy burden." Two others (Stewart and White), while recognizing the "concededly extraordinary protection against prior restraints," nevertheless were willing to allow an injunction upon a showing of "direct, immediate and irreparable damage to our nation or its people."

This Committee's Assessment

As stated, Admiral Inman's criteria suggested, for discussion, legislation which would set up a system of prior review of articles and monographs relating to cryptology. This Committee was formed by ACE to carry out such a discussion. Under Admiral Inman's criteria, such a system would be less objectionable than classic systems of prior restraint that vest in an administrator the legal authority to review proposed publications under discretionary standards and make it a crime to publish them without the administrator's approval. First, Admiral Inman proposed that the criteria for what is proscribed (i.e., what can be "censored") should be narrow. Secondly, NSA's General Counsel proposed as a departure point for discussion that the staff's decision be reviewable by a Board, including cleared persons from outside NSA, with a final decision by the Director. Thirdly, no suppression order could be effective unless ratified by a court after a judicial proceeding. Fourthly, the government would have the burden of proof in such a judicial proceeding. Finally, compensation would be paid to an author whose work was suppressed.

This Group feels that NSA's initiative in commencing a public dialogue is commendable and that the Agency has sought to craft a narrow and constructive solution to a problem that it perceives. We reject, however, the statutory solution that has been proposed for a number of reasons:

- (1) We have not been in a position to assess the seriousness of the threat to the national security posed by the publication of selected articles and monographs on cryptology. Such an assessment would require security clearance of committee members and a deep understanding of cryptographic systems. We were offered such clearance, but this committee, made up of persons heavily involved with other tasks and without staff, was in no position to take on such a heavy work burden. Relatedly, we have no sophisticated idea of the types of information that NSA would seek to suppress — we thus cannot discern the reach of a system of prior restraint or adequately evaluate its justification.

¹⁷Emerson 457

¹⁸Note 11, *supra*.

- (2) We have been in no position to gauge systematically the impact of a statutory prepublication review system on nongovernment research in cryptology or the economic or social losses that a negative impact might entail. Possible negative impacts include loss of scientific advancements and innovations which might lead to better security against invasions of privacy of individuals and commercial entities and enhanced opportunities for foreign trade. It is clear to us that cryptology has become important outside of government as electronic storage and transmission of data enlarge in the private sector.
- (3) We have been unable to fashion a narrow and precise definition of that cryptologic information that should be kept secret. We feel that such a definition is essential to provide adequate notice in order to protect persons from criminal punishment for unintentional violation, to limit the discretion of regulators, and to lessen the inhibiting impact or chilling effect that would attend ambiguous or overbroad standards.
- (4) We are impressed that, without the foregoing definition, a system that punishes publication of scientific and technological information, or subjects proposed publications to legally required prepublication review, is contrary to the values expressed in the legal and political history of the First Amendment.
- (5) From a practical standpoint, any system of prior review will work best with the cooperation of the cryptology community. It seems clear that a voluntary system is likely to generate more cooperation than would a compulsory statutory system.

A Suggested Voluntary Procedure

The committee accepted as a working premise Admiral Inman's concern that some information contained in some articles and monographs could be inimical to the national security. In light of the preceding legal, policy, and practical analyses, we cannot recommend a statutory system of pre- or postpublication review. Under these circumstances, we recommend an alternative nonstatutory system designed to test on an ongoing basis Admiral Inman's hypothesis, which depends for its success on the voluntary cooperation of those whom NSA might seek to regulate. What follows is an outline of such a system that includes an Advisory Committee cleared to a level that enables it to test adequately our working premise on an on-going basis. The implementation of this system will require that NSA convince authors and publishers of its necessity, wisdom and reasonableness. We believe that NSA will be able to be convincing if it establishes a record in its dialogues and its administration that evidences sensitivity, narrow application and remedies, and a sense of restraint and reasonableness to those who are asked to cooperate. We believe that many researchers would welcome an opportunity to find out in advance whether what they plan to publish would directly and substantially risk compromising national security interests.

We realize that any system of prior review involving governmental agencies, even a voluntary one, creates an environment that might dampen the desire of academics and others to undertake research. In view of Admiral Inman's serious representations of threats to

national security, however, we recommend the system here outlined be tried on an experimental basis.

The Study Group also recommends that a timely review be conducted concerning the operations of the recommended voluntary system, should one emerge, and that the relevant professional societies receive and record comments on such operations for use in the future review.

Our recommendation of a voluntary procedure on a trial basis should not, however, be construed as endorsing any legislation that might be modeled on the proposed procedures.

The following guidelines are suggested for the proposed voluntary system:

- (1) NSA would notify the cryptologic community, including authors and publishers, of its desire to review manuscripts concerning aspects of cryptology prior to publication.
- (2) NSA, in consultation with appropriate technical societies, would define as precisely as possible those aspects of cryptology to be covered by the procedure.¹⁹
- (3) NSA would invite authors to send manuscripts to NSA for review prior to publication.
- (4) NSA would assure prompt review by its staff of submitted manuscripts and prompt response to authors with an explanation, to the extent feasible, of proposed changes, deletions, or delays in publication, if any.
- (5) NSA would provide, in the case of unresolved disagreements, the opportunity for authors to obtain prompt review by an Advisory Committee of five persons (two appointed by the Director of NSA and three appointed by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Science), which would make a recommendation to the Director of NSA and to the author concerning the matters in issue. Members of the Advisory Committee shall have adequate clearance so that the committee can make informed recommendations.
- (6) There would be a clear understanding that submission to the process is voluntary and neither authors nor publishers will be required to comply with suggestions or restrictions urged by NSA.

¹⁹There are two problems of definition: (1) stating criteria to identify those articles and monographs which NSA wishes to review; (2) stating criteria to be used by NSA and the Advisory Committee to determine information the disclosure of which would directly and substantially compromise national security interests. Criteria for the first task must be broader than for the second. Nevertheless, care should be taken in both instances to narrow the scope of application to the extent feasible, and both sets of criteria should be published to the greatest extent possible.

The Committee determined to leave the ultimate definitions to NSA in consultation with appropriate technical societies. It believes, however, that NSA at the outset should exclude from review or proscription information concerning, for example, general mathematics, engineering, computer science or statistics, and basic theoretical research.

**THE CASE AGAINST RESTRAINTS
ON NON-GOVERNMENTAL RESEARCH
IN CRYPTOGRAPHY**

George I. Davida

A minority report of the Public Cryptography Study Group
of the American Council on Education

INTRODUCTION

The objectives of this report are to present arguments against restraints on non-governmental cryptographic research. Time and space limitations preclude a complete treatment of the subject of cryptology and the history of the conflict between the National Security Agency and the academic researchers in cryptology. The report of the PCSG contains some of this material.

NSA OBJECTIONS

It is difficult to state precisely NSA's objections to the open publication of research papers pertaining to cryptology and allied areas. In general the NSA claims that its mission will be harmed by such publications. Specifically the NSA claims that

- A. Foreign governments might use the cryptographic results to deny the NSA the ability to perform intelligence gathering.
- B. The basic or applied research results might accidentally lead to compromise of NSA designed cryptosystems.

In the rest of the report the area of cryptology will be discussed briefly and the validity of the NSA's claims will be examined.

CRYPTOLOGY AND ITS IMPORTANCE

While a complete treatment of this subject is not possible in this report, it is important to briefly examine the area and, to put it in proper context, the role it plays in Information Protection (or Data Security).

CRYPTOGRAPHY consists of methods for transforming data, using a key, to render the data unintelligible to someone not authorized to have it. The process of so transforming data is called **ENCRYPTION**. A legitimate user can transform the garbled data back to its original form, using a key. This process is called **DECRYPTION**. **PLAINTEXT** is encrypted into **CIPHERTEXT**.

CRYPTANALYSIS consists of methods that are used to transform encrypted data back to its original form without the knowledge of the key.

Information Protection (or Data Security) pertains to the protection of data processed by, stored in or transmitted by computers. To protect data, a large number of problems must be solved. We shall examine a few of them.

PHYSICAL SECURITY

Obviously the best security methods are worthless if someone could just walk off with data on tapes or disks. Thus the facilities housing the computer system must have controlled access that is effective. These problems are not peculiar to computer security and will not be discussed any further other than to point out that the increasing use of electronic locks involves encryption.

DATABASE SECURITY

This is an area of great concern to the researchers and the public. Martin Hellman, who was the first to express concern about the safety margin of commercial cryptosystems, has said that the United States is the most computerized country in the world and the one to lose the most from insufficiently secure systems.

The increase in the computerization of the society has led to the construction of a large number of databases that are ELECTRONIC WINDOWS into the most intimate details of people's lives. What is even more disturbing is that it is usually impossible to know who is looking in. Thus these databases are like ONE WAY MIRRORS.

Encryption can serve as a curtain. Therefore the need for a civilian (or non-governmental) effort in cryptography is a strong one. Research results have shown that databases used for statistical purposes are subject to compromise. Using harmless-looking queries (questions), such as asking for the AVERAGE income of individuals in certain categories, it is possible to compromise a database.

The use of databases in employment can result in the accumulation of records on individuals containing data that is both performance relevant as well as data that is subject to privacy protection. The only effective methods for maintaining separation of such data involve encryption. (Preventing the collection of data of certain types is not feasible.)

OPERATING SYSTEM SECURITY

Operating systems are computer programs that perform a large number of functions among which are: 1) the management of resources attached to a computer (such as tapes, disks, memory, files, programs, messages, etc.) 2) allowing several users to compute simultaneously on the same computer.

These tasks are very complicated. Insuring that access to resources is proper (from a security viewpoint) is a problem that has not been satisfactorily resolved. Operating systems may have loopholes that may allow a user to gain access to resources that are supposed to be inaccessible.

The importance of encryption in the design of secure operating systems is demonstrated in the recent design proposals for secure systems.

COMMUNICATION SECURITY

This is the most well understood of the sub-areas of information protection. Historically data was most vulnerable when it was transmitted (or communicated) in some way. Until recently this was the main area of application for encryption. This has changed. New problems in protection of data during communication have arisen that greatly affect the average person in day-to-day activities. The emergence of COMPUTER NETWORKS has led to new applications that threaten privacy to a degree that was not possible before. For example, as the credit card operations go "on line", (i.e., gain instant access to a computer that can authorize the charge or service), suddenly, data that was more or less unavailable before is put on communication lines.

New applications, such as Electronic Mail and Electronic Funds Transfer, require the use of encryption. Other applications, such as those in personal computing, will continue to be discovered as computers proliferate.

RESTRAINTS

The ACE PCSG began by considering the recommendation of model legislation for PRIOR RESTRAINT on cryptology papers. The committee's decision to go ahead and recommend restraints (first mandatory and later voluntary) had no basis whatsoever.

The following constitute some of the arguments against restraints:

- I. The National Security interests of the country are considerably broader than the narrow mission of the NSA, which in a nutshell is DATA GATHERING.

The PCSG refused to address the question of whether the broad interests of the country (which include such things as Privacy Protection) would outweigh the risks (*if any*) to the NSA's mission. The committee felt that this was too abstract an issue. The importance of Cryptography to telecommunication protection as well as other computer security areas (outlined above), however, is as concrete an issue as one could hope to get. The need for a non-governmental effort in this area is crystal clear in view of the remarkable insensitivity of the common carriers to the public's concern about privacy. The reported foreign intelligence activities in this country against individuals (or corporations) attest to this. As it was pointed out above, the increase in the level of computerization heightens the need for a cryptographic effort independent of the government.

2. Restraints would adversely affect the quality and direction of basic research in computer science, engineering, and mathematics.

The impact of any types of restraints on research (either applied or basic) was not adequately addressed by the committee. The effects of withholding basic or applied research results relating to cryptography would handicap researchers, not only in data security, but in computer science and engineering and allied areas. The restraints would remove from the public domain the most interesting and intellectually stimulating results. The long-term consequences would no doubt be harmful to the Nation.

Consider the problem of implementation of restraints. It has been suggested that the test for whether a paper should be withheld from publication might be "the degree of significant use" of a cryptosystem. A case in point is the use of the Rivest-Shamir-Adleman cryptosystem in the Zero Power Plutonium reactor. The security of this system depends on the fact that no efficient methods for factoring a large number have been found. In view of the recent results related to this problem, some researchers now believe that such methods might indeed be found. If that were to occur, then a solution might have to be suppressed since some can argue that the application just mentioned constitutes a significant use. The solution to an age-old problem would thus be withheld from researchers.

3. Restraints would be unconstitutional.

The constitutionality of restraints was only glossed over. It was pointed out that in one case where legislation did exist (the ITAR) the Justice Department had issued an opinion that that was unconstitutional. It was suggested that the Justice Department opinion on ITAR was in dispute.

4. Restraints, the implementation of which is to include the cooperation of editors of journals, would cause international complications.

The technical societies that publish the journals would have serious problems with having to cooperate with the NSA. They may find themselves subjected to harassment by other governments since many of the societies are international in scope. This would have an effect on the scientific exchanges, treaties, and understandings. (For example, it might affect such things as what journals constitute "intelligence" journals.) It would set precedent for the discussions on the freedom of the press that are conducted elsewhere. There may very well be an impact on the Transborder Data Flow guidelines recently concluded.

Finally, the journals may find it impossible to carry out the implementation of such restraints because their charters would not allow it.

5. Restraints would lead to legal entanglements with existing laws.

Restraints may put the researchers in a very difficult position with respect to the laws that already exist:

- a. The impact of restraints on the patent secrecy process is significant. The restraints would enhance the government's ability to issue these orders.

If the restraints were to be put in effect, then an applicant for a patent based on the now unpublished result would risk a secrecy order since existing law disallows the government from issuing a secrecy order when the subject matter had been published in the open literature.

- b. Researchers may find themselves violating state statutes if they were to comply with restraints.

The committee did not address the potential impact of restraints on existing laws. Since research in most cases is funded in part by state funds, a researcher may not be able to simply drop some results from his/her paper for nontechnical reasons.

6. Restraints, even if desirable or possible, would be ineffective in achieving the NSA's objectives.

The very nature of Cryptography makes it unlikely that restraints would be effective barriers to TECHNOLOGY TRANSFER. Cryptography is not hardware intensive. The main hardware needed for implementation is a microprocessor, an abundantly available and inexpensive device. This means that the restraints would be placed on an activity that is largely intellectual — design and analysis of algorithms.

Since the hardware involved in the design of cryptosystems is not controlled, the restraints would result in removing from the public domain the most interesting algorithms, thus seriously handicapping the researchers in this country. Researchers in other countries, who are not likely to have such restraints, would be quite capable of designing their own algorithms. **THEY WOULD ANYWAY!!** The design of cryptosystems involves a large degree of distrust and suspicion about the possibility that a system will have a shortcut known only to the designer. Thus, as David Kahn has said, governments are unlikely to trust anyone but their own scientists and engineers. One can even argue that if in fact they were to use the systems designed in this country, then that would present opportunities for intelligence gathering.

7. The likelihood that basic research results would lead to efficient cryptanalytic attacks against the government's cryptosystems is practically nil.

The NSA claims that the basic or applied research results might lead to efficient attacks against the systems that they have designed. This is not likely because *researchers do not engage in cryptanalysis*.

Cryptanalysis is a tedious and time/resource consuming activity. Inverting a cryptographic function is not that attractive. These mathematical functions are for the most part "ugly" functions that, even if inverted, could be made just as difficult by a change of one or two symbols. Thus the intellectual attraction is not there. Furthermore, researchers do not have access to NSA's cryptosystems. The analogy that Martin Hellman used was that of a chemist inventing a chemical such that a drop would eat through a Sherman tank. The likelihood of such an occurrence is of course high if the tanks were made of plastic. Besides, the very concept of denying the public the opportunity to advance in a field just to enable the NSA to perform its job is alien to the traditions of this country.

REMARKS

While the PCSG has retreated from recommending model legislation, its actions are still troublesome. The very recommendation that restraints be put into effect, even if voluntary, is dangerous. There already is talk of a trial period to see if the NSA is happy about the outcome. There is clear indication that if the NSA is not, then legislation will be sought. At that time, this committee's recommendation could be used as expert testimony that NSA's claims are valid. Such a conclusion would be erroneous. The majority of the committee members are not researchers in data security or cryptography or computer science or engineering.

In conclusion, I find NSA's effort to control cryptography to be unnecessary, divisive, wasteful, and chilling. The NSA can perform its mission the old-fashioned way: STAY AHEAD OF OTHERS.

ACKNOWLEDGMENTS

I would like to thank the following individuals, with whom I have had a number of discussions on this subject:

David Kahn, Carl Hammer, Martin Hellman, Ronald Rivest, Len Adleman, Gutavus Simmons, W. Richards Adrion, Richard Lipton, Richard DeMillo, Whitefield Diffie, Ralph Merkle, David Watters, Charles Wilk and Gerald Sturges.

AMERICAN ASSOCIATION OF UNIVERSITY PROFESSORS

ONE DUPONT CIRCLE - SUITE 500
 WASHINGTON, D. C. 20036-1179
 Telephone 202-466-8030

President

Victor J. Stone
 University of Illinois
 at Urbana - Champaign

October 31, 1983

General Secretary

Irving J. Spitzberg, Jr.
 Washington Office

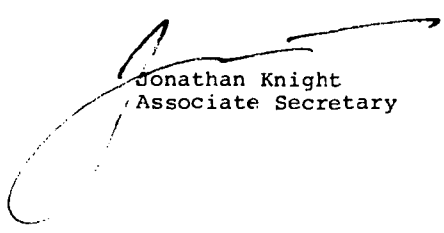
Mr. David Beyer
 House Subcommittee on Courts,
 Civil Liberties, and the
 Administration of Justice
 2137B Rayburn House Office
 Building
 Washington, D.C. 20515

Dear David:

Here are the three reports which we have issued during the past eighteen months concerning restraints by government agencies on academic freedom. "Government Censorship and Academic Freedom" will appear shortly in our journal Academe: Bulletin of the AAUP. The report was also submitted as testimony before the House Subcommittee on Legislation and National Security, which held hearings on October 19 concerning the Presidential Directive on Safeguarding National Security Information.

With good wishes.

Sincerely,



Jonathan Knight
 Associate Secretary

JK/ps

Enclosures

GOVERNMENT CENSORSHIP
AND
ACADEMIC FREEDOMIntroduction

Within the past year, the American Association of University Professors has issued two reports which discuss the ramifications for academic freedom of restraints by government officials on the open circulation of ideas.^{1/} Changes have been urged in the direction of limiting the impact of these restrictions upon scholarship and research, but to no discernible effect. Instead, there has been a significant enlargement of the scope of government restraints. These include:

1. Decisions by Department of State authorities to deny visas to foreign academics invited to attend scholarly meetings in this country on the basis of their political beliefs or associations.

2. A regulation proposed by the Department of Energy to require any holder of unclassified information relating to nuclear energy to assure the government that this information is protected in a manner similar to other restricted materials in its possession.

^{1/} "Federal Restrictions on Research: Academic Freedom and National Security," Academe: Bulletin of the AAUP (September-October, 1982), pp. 18a-20a, and "The Enlargement of the Classified Information System," ibid (January-February, 1983), pp. 9a-14a. An abridged version of the second report appeared in Science (21 January 1983), vol. 219, pp. 257-259. For a useful survey of the several actions taken by the current administration to impede the free flow of unclassified ideas see Floyd Abrams, "The New Effort to Control Information," The New York Times Magazine, September 25, 1983.

Stanford University has estimated that the regulation would apply to an unknowable portion of the some five million volumes in its libraries.

3. Executive Order 12356 (April, 1982), which extended the reach of the government's system for classifying information on the basis of national security concerns by relaxing the standard according to which the determination of classification is made. The likely result of this change is to remove from public and scholarly access additional tens of thousands of items that bear upon one's ability to determine the truth of statements made by executive branch officials, as well as upon the integrity of one's own work. The executive order also enlarged restrictions interdicting publication of research that is "born free" but that may, under the order, "die classified." It enables executive branch agencies to halt the presentation, publication, or mere scholarly exchange of papers not classified and not drawn from any classified sources.

It is plain that government officials are already intruding upon freedom of inquiry and academic research on a significant scale. And now, the most recent executive initiative, the Presidential Directive on Safeguarding National Security Information (March, 1983), the subject of the present report, proposes to add even more to these stringent measures.

Summary of the Presidential Directive's
Prepublication Review Procedures

The Directive provides that each agency of the executive branch will adopt internal procedures to assure minimally that "all persons" who have access to highly classified intelligence information will sign a prepublication review agreement to "assure deletion of . . . classified information." The Directive does not identify what is to be reviewed by the government agency or for what period of time a person is required to comply with the prepublication review agreement. Considering the emphasis that this administration has placed on restraining the dissemination of unclassified information and the broad language in which the Directive is cast, it seems entirely possible that government agencies will view the Directive as encompassing all writings by those with access to classified information for however long these individuals seek to publish what they write.^{2/}

The Directive is silent with respect to whether it shall be applied only to those with current access to classified information. A government agency could presumably assert the need to review the writings of someone who no longer has a security clearance for whatever period of time the agency deems prudent.

The reason for the system of prepublication review to be established under the Directive is stated thus: "Safeguarding against unlawful disclosure of properly classified information is

^{2/} The General Accounting Office has reported that 112,660 federal employees (this figure does not include the Central Intelligence Agency and the National Security Agency) and 15,090 federal contractors currently have access to this classified intelligence information. During 1982, the GAO identified the following types and quantities of information reviewed during the prepublication process: 68 books, 7,805 articles, 2,889 speeches, and 92,918 pages not identified.

a matter of grave concern and high priority for this Administration."^{3/}

Sanctions can be applied to persons who, subject to a prepublication review agreement, do not submit everything which they may write to the government agency for prior review.

In addition, the Directive provides that government employees can be required to submit to polygraph examinations as a condition of employment, although the polygraph itself is of doubtful reliability, its use is widely feared, and submission to the examination may be required without regard to a stated probable cause and without any clear limits respecting the questions to be answered.

In sum, the effect of the Directive is that government officials may require anyone with current or lapsed access to high-level classified information to submit any writing intended for publication to the government agency for prior review. Those who have ever had access to classified information would accordingly, we take it, be placed indefinitely under the constraints of government censorship.

^{3/} The Department of Justice chaired the interdepartment group which drafted the Directive. In a fact sheet released upon the issuance of the Directive, the Department of Justice stated that "Unlawful disclosures of classified information damage national security by providing valuable information to our adversaries, by hampering the ability of our intelligence agencies to function effectively, and by impairing the conduct of American foreign policy."

Observations

The exercise of academic freedom by teachers and scholars requires freedom of thought and expression within colleges and universities and the freedom to transmit the fruits of inquiry to the wider community. To an increasing extent, society in general and government in particular have come to rely upon academic researchers for acquiring new skills and new knowledge. Plainly what is published by academic researchers also serves to enhance public discussion of political issues. Without the liberty to explore and the correlative right to publish the results of research, academic freedom and the advancement of learning are impaired.

Within the academic community a researcher freely submits a manuscript to colleagues and other qualified persons for their judgment and evaluation. The assessment by peers gives confidence to the researcher of the usefulness of a path traversed. It can also warn against possible error or unnecessary duplication of research efforts. The exchange of criticism and ideas is also an indispensable condition for the continuance of research itself. The investigator's communications with peers may yield new insights or lead to research programs not thought possible or even imagined.

Free thought and free expression are significantly injured if researchers are unable to disseminate the results of their research and to publish what they have discovered except upon con-

dition that their writings are to be submitted to a government agency for prior review. The concept of academic freedom necessarily embraces the freedom to impart the findings of inquiries without previous restraint or fear of subsequent punishment.

The Directive cannot be justified on grounds that the system of prior review would not be onerous or that in practice few writings would be materially altered.

Each year countless numbers of professors representing a wide range of academic disciplines serve the government in various capacities. Some serve as consultants, lecturers, or researchers. Others accept short-term government assignments, in this country or abroad, while retaining their faculty appointments. Still others resign their academic positions for a government post and return to the teaching profession years later. There are also those who accept faculty positions after serving in government for varying lengths of time. Many among these faculty members are given, or once had, access to classified information. To accomplish what the authors of the Directive seek, and with consideration of the sheer numbers of academics and other persons with access to classified information, government agencies would need to establish a vast apparatus for administration and enforcement.

In addition, a system of prior review could not be limited only to those writings that a government agency is likely to identify as harmful to the nation if revealed to the public. A government official cannot be certain in advance of examining a manuscript

whether it contains sensitive information. A probable result is that the Directive would be administered to review a broader area of expression than might be restrained through actual revision or deletion of restricted information. One can also expect substantial delays in reviewing manuscripts, owing in part to the complexity of the undertaking and in part to the likely controversies between government agencies and authors concerning whether and how to alter a manuscript.

There is also reason to doubt the circumspection of government officials responsible for implementing the Directive. In 1970, a Department of Defense Task Force on Secrecy concluded that the amount of scientific and technical information which was classified could be profitably decreased by at least 90 percent. A report released by the General Accounting Office in 1979 found that nearly twenty-five percent of the classified materials it had reviewed contained one or more instances of improper classification. From the perspective of a government official accountable for failing to classify information that might be used to the detriment of the nation's security interests, the necessary choice in deciding whether or not to classify is to err overwhelmingly in the direction of classification. Only by accepting the premise that most information reviewed for classification should be secreted, whatever its actual adverse effect on national security if released to the public, can a government official discharge the responsibility of insuring that no information that should be classified will escape classification.

The factors accounting for mistaken classification would all too likely exercise their baleful influence under the Directive's system of prepublication review.

The process of administering the Presidential Directive will thus be piled on top of a system of classification which is already excessive, is already seriously compromising of academic freedom, and is known for its susceptibility to executive manipulation.

Moreover, the mere existence of the Directive is repressive. We want scholars to be uninhibited in challenging traditional habits of thinking, in testing new theories, in criticizing social and political institutions, and in advocating change in the policies and programs of government agencies and officials. The executive branch, the Directive asserts, may not curtail freedom except when it finds it advisable to do so. Yet uncertainty as to whether any particular manuscript should be submitted to a government agency for prior review can only inhibit the pursuit of intellectual and political truth. It is not merely that useful research may be frustrated. Rather, it is that the intimidating character of the Directive undermines the true foundation of our national security, the common confidence that things are as they seem and that our government's policies are not tragically misconceived on facts that are actually falsehoods.

The Directive can also be expected to take its toll by reducing the willingness of academics to accept government responsi-

bilities. Many will conclude that the diminution of their freedom is too great a price to pay for the opportunity to serve government.

The government claims, of course, that it is concerned with avoiding harm to the national security. If the broad reasons invoked in the Directive are a valid justification for the policy, then the executive branch would have complete discretion to determine what are any justifiable ends and could restrain manuscripts accordingly. Even if credit is given to the administration's position that the dangers it warns against are significant, two further issues arise.

The Directive seeks to prevent the unauthorized publication of classified information through a system of prior review. A claim to immunity from restraint is not unlimited. National security certainly requires secrecy in some areas, and the government must have the means to protect the nation against the wrongful disclosure of military secrets. It is equally certain, however, that procedures for restraining free expression, to the extent that any are required, must be precise, narrowly defined, and applied only in exceptional cases, for otherwise the exercise of the freedom would have slight value for the purpose it is meant to achieve. These limitations are not to be found in the Directive. The reach of the Directive is without parallel in modern memory. It may be applied to the writings of thousands of persons, whether or not

they are serving in government, who currently have or did have access to classified information. We do not find credible that any genuine problem faced by the administration in controlling the distribution of classified information can justify the unbridled sweep of this Directive.

We also question whether the dangers invoked by the administration in justifying the Directive are more pressing than those of the recent past. We would do well to remind ourselves of some crises through which the nation has passed since the end of World War II.

Each day for nearly a year the immediate prospect existed that American and Soviet troops would come to blows during the Berlin Blockade. That possibility was seriously revived with far vaster implications during the Cuban missile crisis. We fought two wars on the mainland of Asia, and neither in Korea nor in Vietnam were our apprehensions about the intentions and capabilities of the Soviet Union less acute than they are today. And the revolution in Iran and the Soviet Union's invasion of Afghanistan not only deprived us of intelligence stations on a large stretch of the border of the Soviet Union but for many raised the threat of a Soviet thrust toward the Persian Gulf and the undermining of the entire American position in the Middle East.

What greater urgency propels our current administration? We must continue to contend with a formidable adversary, but why should the same principles which have governed free inquiry by

academic researchers not be found serviceable in these anxious times? We make a fatal bargain if we allow the freedoms which have so long been exercised in this country to the benefit of all to become diminished, whatever the concerns which are now motivating some government officials.

The Directive should be withdrawn. Its infirmities are too many and they run too deep to be cured with textual refinements. Our penchant for executive secrecy is not in our own or in the world's best interest. We should be striving for reliable ways of reducing the government's system of classification to a bare minimum, and not for excuses for its protean enlargement.

Robert A. Rosenbaum (Mathematics)
Wesleyan University, Chairman

Morton J. Tenzer (Political Science)
University of Connecticut

Stephen H. Unger (Computer Science)
Columbia University

William Van Alstyne (Law)
Duke University

Jonathan Knight, Staff

*American Association
for the Advancement of Science*

1515 MASSACHUSETTS AVENUE, NW, WASHINGTON, D. C., 20005

Phone: 467-4400 (Area Code 202)

Cable Address: Advancesci, Washington, D. C.

October 1983

PROJECT ON SECRECY AND OPENNESS
IN SCIENTIFIC AND TECHNICAL COMMUNICATION

SPONSORED BY
AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE
COMMITTEE ON SCIENTIFIC FREEDOM AND RESPONSIBILITY

In recent years, the traditional concept of scientific ideas and information as a public good, freely available to professional colleagues as well as the general public, has come under closer scrutiny. The post-World War II increase in the economic, political, and military value of scientific and technical information has fostered various private and public proposals to restrict open communication in university teaching and research activities. These proposals have cited many justifications, including national security interests, economic competition, patent protections, and quality control, as the basis for limiting access to new and important research data in selected fields.

Conflicts over secrecy and openness in science are essentially conflicts over values. In order to explore the fundamental values which promote secrecy or openness in science, the American Association for the Advancement of Science has initiated a new project through the office of the AAAS Committee on Scientific Freedom and Responsibility. The project, titled "Secrecy and Openness in Scientific and Technical Communication" is supported by a grant from the Program on Ethics and Values in Science and Technology (EVIST) in the National Science Foundation, and the Humanities, Science and Technology Program in the National Endowment for the Humanities. Ms. Rosemary Chalk, Program Head for the AAAS Committee, is the project director.

The tradition of openness in research is the foundation for objectivity in science. It is through the free exchange of information and data that new ideas and experimental results are subjected to the rigorous test of peer review and verification. The origins of openness, however, have

their roots in a period when science was essentially a private intellectual activity. Also, many scholars are not completely "open" in their exchange of data and information. Self-imposed restrictions on the release of new but unconfirmed theories or preliminary experimental data are quite common in traditional scientific work. These restrictions, which form part of the ethos of science, are themselves limited by notions of fair play and equity, however, and are subject to abuse when stimulated by objectives other than the protection of incomplete work.

In modern times, government, industrial and university groups have increasingly recognized the importance of applying scientific and technical resources to selected public and private objectives. Access to new information, including basic research, has emerged as a source of competitive advantage in the pursuit of various social, military, and economic goals. As a result, the concept of intellectual property has expanded in the post-World War II period to justify occasional controls on the disclosure of basic research findings supported by public or private funds.

For example, in a series of reports describing concerns about technology transfer leaking advanced U.S. technology to foreign adversaries, the Defense Department has questioned whether the openness associated with university research in areas of direct military application is detrimental to national security interests in a time of escalating East-West tensions.

In the commercial area, a number of firms are exploring arrangements whereby universities can develop research projects and academic programs suited to the needs of particular industries. Within such arrangements, one major source of concern and controversy is pre-publication review of, and patent protection for, new research data resulting from industry-sponsored work.

Secrecy also results from actions within the scientific community. As personal prestige, professional advancement and financial gains become more closely tied to publication, some individual scientists have indicated reluctance to exchange new research findings or materials with colleagues and students in the traditional manner.

These public and private pressures foster secrecy in science. Such restrictions on communication often serve legitimate and important social purposes. They may at times also result in arbitrary or abusive practices, or promote bias and the loss of objectivity in research.

Although there is reason to believe that secrecy is increasing in science, and that it may affect values other than openness, very little is known about the ways in which secrecy or openness influence the conduct of scientific research. It is for the purpose of encouraging attention to such relationships, and the values which affect professional behavior and education, that the AAAS Committee on Scientific Freedom and Responsibility has initiated the new project.

The AAAS project will consist of a series of background papers and regional seminars to be organized in 1984. Ten background papers will be commissioned through the project. Five project seminars will be held in Boston, and one each will be held in Chicago, Nashville, San Diego and Washington, D.C. A project symposium will also be held as part of the 1984 AAAS Annual Meeting in New York.

Co-sponsoring institutions are:

American Association for the Advancement of Science, Committee on Scientific Freedom and Responsibility

Center for the Study of Ethics in the Professions, Illinois Institute of Technology (CSEP/IIT)

Management of Technology Program, Vanderbilt University

Program in Science, Technology and Society, Massachusetts Institute of Technology (MIT)

Science, Technology and Public Affairs Program, University of California, San Diego (UCSD)

Science, Technology and Human Values

Regional hosts for the project are: Rosemary Chalk, AAAS project director, Washington, D.C.; Robert House, director, Management of Technology Program, Vanderbilt University; Marcel La Follette, editor, Science, Technology and Human Values, MIT; Sanford Lakoff, professor of political science, UCSD; and Vivien Weil, senior research associate, CSEP/IIT.

Advisory committee members guiding the development of the AAAS project are: Loren Graham, professor of the history of science, MIT; Harold P. Green, professor of law, George Washington University; Lee Grodzins, professor of physics, MIT; Louis Menand, senior lecturer in political science and special assistant to the provost, MIT; and Eugene Skolnikoff, director of MIT Center for International Studies.

Further information about the project can be obtained from Rosemary Chalk at the AAAS address, or call (202) 467-5238.

*American Association
for the Advancement of Science*

1776 MASSACHUSETTS AVENUE, NW, WASHINGTON, D. C., 20036

Phone: 457-4400 (Area Code 202)

Cable Address: Advancesci, Washington, D. C.

February 15, 1984

The Honorable Robert W. Kastenmeier
Chairman, Subcommittee on Courts,
Civil Liberties and the
Administration of Justice
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

Your letter of November 16, 1983, invited my views on the civil liberties implications of restrictions on scientific communication.

As you know, science has no quarrel with national security. For some forty-five years, through hot and cold wars, science has provided the means for technical superiority to our defense forces. The key to the government/science partnership has been trust, a trust to which each partner has been committed.

Government now seems to be retreating from that basic proposition. Impelled by perceptions of the Cold War and a military vulnerability gap, key government officials are trying to deny U.S. scientific and technical assets to adversary countries. In doing so, government has resorted to security classification of scientific research, broadened its powers of classification, employed contracting powers to compel prior restraint on scientific reporting, publishing, and conferring, and carried out pre-emptive raids on scientific meetings where unclassified research and development progress would be discussed in the possible presence of non-U.S. citizens. In addition, government is extending visa refusals to foreign visitors, and demanding that universities police the activities of foreign students who are engaging in unclassified basic research that might bear some relationship to future national security affairs. Mutual trust does not prosper in such a policy environment. Nor does science progress.

If these policies prevail beyond the short term, the consequences are predictable. Because science is a discovery process, it relies fundamentally on the circulation, replication, and transfer of experimental results. This process keeps science honest and accountable. It defines the merit, or its lack, of research findings. Science does not tolerate either fraud or incompetence. That, in itself, is what government depends upon -- the self-policing function of the scientific process. But under

a system of governmental surveillance, prior restraint, and the implied threat of withholding research support, the tendencies will be towards knuckling under to government's terms and conditions; towards conservatism; away from the risk-taking that drives the best science; towards pursuing the kind of research that seems safely out of the field of governmental interest; and towards avoiding the sanctions that accompany government's contracts, grants, and research agreements. Mediocrity in science is sure to follow. When it does, the U.S. lead in science cannot last.

What is especially troubling about the present government's approach to national security in this context is its lack of selectivity. There is no disagreement on the part of the scientific community that some areas of research and development are highly sensitive and should be safeguarded carefully. This approach is called "building tall fences around narrow areas," as outlined in the Bucy Report a decade ago. There is general agreement with the practices of security classification where the research is weapons-related. There is substantial agreement that dual-use high technology is an appropriate area for selective safeguards.

But government's approach is not selective. It is a "safety net" approach that seeks a zero-free result, and scientists have no way of knowing when their unclassified work is going to be ambushed by a government employee who rarely has the professional knowledge to understand the scientist's work. And it is this aspect of government's approach that undercuts the factor of the scientist's trust in the fairness of the government partner.

The way to resolve this conflict situation is not to give government a blank check to classify or otherwise restrict whatever it chooses, in an atmosphere of secrecy. It is not good public policy to employ the Defense Department's contracting powers on a wall-to-wall basis by imposing universal obligations upon researchers to submit to prior review and approval of all research publications or reports. It is not a workable public policy to formulate a list of militarily-critical technologies consisting of thousands of items. It is not good policy to put scientists or university administrators at risk for participating in the normal international flow of scientific discourse.

Government has made no case that the national security has been damaged by the free disclosure of unclassified university-based scientific research. In secret briefings, on the other hand, government has made a case that technological assets have been leaked away to the advantage of the Soviet Bloc, mainly through legitimate and illegitimate trading arrangements together with deliberate espionage.

The issue goes to the appropriateness of imposing unworkable restrictions upon unclassified research in universities and industry, and to whether the costs to scientific and economic productivity do not exceed the marginal benefits to our national security interests. But at a higher level

of concern, what is at stake is the prospect of a serious rupture in the quality of government's postwar partnership with science, and this question should not be left to the Department of Defense to decide. It is decidedly the business of the Congress, in dialogue with the Executive Branch and the scientific community.

The Congress should be wary of extending the powers and authorities of the Executive Branch through overly restrictive provisions of the Export Administration Act. It should examine the performance of the Department of State in applying discretionary criteria in the administration of visa functions. It should spell out, in legislation, the tests that executive agencies must meet before imposing burdensome prior restraints on scientific communication in unclassified research. It should appropriate enough money, at the same time, to assure effective enforcement of export controls on embargoed high technology.

What is no less important is that the Executive Branch make its rules clear and understandable to the scientific community, and to have a consistent government-wide set of rules in place of the disarray that presently prevails.

Your interest in these matters is very much appreciated.

Sincerely,



William D. Carey
Executive Officer

WDC:11

YALE UNIVERSITY
NEW HAVEN CONNECTICUT

OFFICE OF THE PRESIDENT

December 12, 1983

The Honorable Robert W. Kastenmeier
U. S. House of Representatives
2232 Rayburn House Office Building
Washington, D. C. 20515

Dear Representative Kastenmeier:

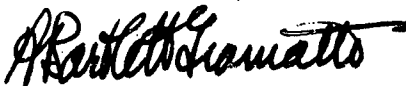
As president of a university whose mission is the advancement and transmission of knowledge, I have been troubled by the restrictions placed by the federal administration in recent years on the exchange of ideas between American and foreign scientists.

These restrictions on the communication of unclassified research data have been made in the name of national security, but in almost every instance a compelling argument can be made that our national security has been harmed, rather than served, by such measures. In large part, this country's economic vitality and military power stem from the productivity of its scientists, and this productivity is heavily dependent on open communication between scientists all over the world. Only when scientific research is designed to meet specific military goals, is security justified, and in such cases the research projects should be classified in advance.

As you know, a panel sponsored by the National Academy of Sciences and chaired by Dale Corson conducted a detailed study of this problem in 1982. I strongly endorse that panel's conclusions and recommendations, which include a number of criteria to be met before any restrictions -- and then only limited ones -- are placed on the dissemination of unclassified data.

I urge that the Congress, under the leadership of your Subcommittee, take the initiations necessary to implement the recommendations of the Corson Panel. In essence, the burden of proof should be placed on the federal administration to show that there is conflict between national security and the open communication of scientific knowledge.

Sincerely yours,



A. Bartlett Giamatti

ABG:rcm



Public Policy Report

FREE SPEECH, 1984

**The Rise of Government Controls
on Information, Debate and Association**

INTRODUCTION

The First Amendment is the bedrock of our democratic system. It reflects our belief that, in a democracy, people ought to have a say in the decisions that affect their lives. It encourages the free flow of information, and is intended to assure that no important governmental policy decisions are made without open and robust public debate.

For this reason, the First Amendment has always come under attack from those in government who would rather make and implement their decisions without bearing the burden of persuading the citizens they represent. Until very recently, most attacks on First Amendment rights were obvious and crude. Demonstrations and parades were prohibited by various local laws; people distributing leaflets or making speeches were often arrested; advocates for various causes were prevented from setting up information tables on the sidewalk; meetings and other public assemblies were broken up.

A great many of these problems persisted into the late 1960s. The civil rights movement, first in the South, and then elsewhere in the nation, confronted many of these laws and practices. So did the anti-war movement during the years of our involvement in Vietnam.

As a result, many laws and practices that crudely restricted First Amendment rights were challenged in court. Most of those challenges were successful, and today the right to meet and to speak, the right to leaflet and to demonstrate are relatively secure. We don't often confront such direct restrictions on these rights anymore, and when we do, we can usually obtain a remedy swiftly and effectively.

Now we face what might be called a second generation of First Amendment problems. Where once the primary means of

suppressing robust debate was to employ crude restrictions on the rights of assembly and speech themselves, today those who would suppress debate seem perfectly happy to permit people to talk and meet to their hearts' content, so long as the content of their speech is strictly controlled. The procedural rights to speak, publish, hear and read remain intact. But what we are permitted to speak about, publish, hear and read is increasingly limited to what the government wants us to know.

The effort to restrict, control and manipulate information that should be available to the public is now emerging as the principle threat to First Amendment rights.

*Information and ideas coming into our country are restricted by licensing foreign books and periodicals, by barring travel to certain countries, and by refusing visas to foreign scholars whose views the government does not want Americans to hear.

*Information and ideas leaving our country are restricted by attempts to control the publication of scientific research and limit the education of foreign students.

*Information and ideas circulating within our country are restricted by expanding the executive branch power to censor ex-employees, by defining too broadly what can be classified, and by placing limitations on the Freedom of Information Act.

Not all these attempted restrictions have been successful. But all of them have been attempted. Those in government who support such restrictions do not share the vision reflected by the First Amendment. They are possessed by a different and more fearful vision. They see the free flow of information as a threat, and seek increasingly to insulate governmental decisions from public debate.

While this trend began before 1980, the Reagan Administration has accelerated it enormously and seems to regard restrictions of information as a central strategy of government. Commenting on the denial of visas to certain controversial speakers,

Representative Fortnoy H. Stark, D of California recently commented: "I'm beginning to believe that the Reagan Administration thinks it cannot survive criticism or free discussion of important issues." Two weeks later, commenting on the Reagan Administration's restrictions of information flowing to Congress, Senator Joseph R. Biden of Delaware said: "Everything is just closing down. The whole attitude is just very, very different."

This report documents that change in attitude and the alarming array of executive branch actions that have been taken recently to restrict the free flow of information and ideas.

These executive actions do not have the drama of a Bull Connor breaking up a demonstration with police dogs and firehoses. No one is arrested. No one is prevented from speaking. Everything seems legal. But that is where the danger lies.

The new tactic of suppression is much quieter, almost stealthy, more difficult to see and therefore harder to resist. But it is nothing less than a covert action against the First Amendment and, ultimately, democracy itself.

Ira Glasser

Executive Director of the
American Civil Liberties Union

I. GOVERNMENT SECRECY

Information is power. Without information, a democratic citizenry cannot exercise its rights, even if such rights continue to exist on paper. One has only to look at such repressive regimes as South Africa, Poland or Uruguay, where state censorship is practiced on a massive scale, to appreciate the importance of the free flow of information from the government to the people and back again.

But a hallmark of the Reagan Administration has been its fear of and hostility towards open government and the unrestricted communication of ideas. A relentless campaign to control information has been in progress since President Reagan took office. This campaign is intended to stifle public debate and dissent on controversial issues such as nuclear arms control, covert operations in Latin America, and the protection of our environment. It is intended to insulate government decisions on these issues from the give and take of public debate, and to reduce the obligation of the President to persuade Congress and the public of the policies he wants to pursue. It is essentially an anti-democratic campaign.

FREEDOM OF INFORMATION ACT "REFORMS"

ITEM: "If the Freedom of Information Act is rescinded or crippled, the American people will have been treated as spies for a foreign enemy Do not poke our eyes out or plug our ears."
--Kurt Vonnegut, FOIA Symposium

The Freedom of Information Act (FOIA) was enacted by Congress in 1966 and represented an historic break with the past. No longer would open government be the exception rather than the rule. Under the FOIA any person was entitled to request access to any identifiable record for any reason. In the post-Watergate

year of 1974, Congress amended the Act to make it even more responsive to the public's right to know what its government was doing. This further liberalization of the FOIA led to the release of important information about the massive FBI and CIA surveillance of domestic dissidents during the 1960s and 70s, the testing of dangerous drugs on humans, the dumping of hazardous wastes in populated areas, and the CIA plots in Chile and Cuba.

The pendulum soon began to swing back again towards secret government, and this trend was greatly accelerated with the entrance of the Reagan Administration.

First, Attorney General Smith revoked the 1977 guidelines issued by his predecessor Griffin Bell, who had instructed government agencies to release the information being sought unless it was clear that disclosure would be "demonstrably harmful."

Second, the Administration, in October of 1981, offered up a bill to "reform" the FOIA which would have gutted the Act. Its provisions would have:

- permitted agencies to charge requesters for "overhead" costs and grant fewer fee waivers;
- permitted agencies to grant themselves time limit extensions of more than three months;
- eliminated "de novo" judicial review in national security cases;
- prohibited courts from disclosing affidavits submitted "in camera" by the Government;
- required courts to stay any order for disclosure pending final judicial resolution of any appeal;
- permitted agencies to deny access to any items in their files that are "otherwise available in public records";
- exempted manuals, instructions and examination materials without any showing of harm from disclosure;
- required agencies to deny access to any "business information" if its disclosure "could" impair the legitimate "business interests" of any person;
- exempted materials on "personal privacy" grounds whenever "the detriments of disclosure are not outweighed by its benefits to the public interest";

- exempted any investigatory information "relevant to or used in an ongoing investigation of enforcement proceeding";
- exempted records that would "tend to disclose" the identity of a confidential source;
- exempted any information "maintained, collected or used in" any investigation of organized crime, terrorism, or foreign counterintelligence without any showing of harm from disclosure;
- exempted records "given to the United States in connection with the settlement of a legal action in which the United States is a party or has an interest;"
- prohibited a party to any previously instituted ongoing judicial proceeding (civil or criminal) from requesting records relating to the subject matter of such proceeding;
- permitted agencies to require a declaration by a requester stating on whose behalf the request is made and that the requester or the person on whose behalf the request is made is not barred from making the requests.

Third, on January 7, 1983 the Reagan Administration issued a new policy guidance memo to the heads of all federal agencies and departments on the subject of FOIA fee waivers. The fee waiver provision was enacted in 1974 to prevent agencies from charging excessive fees to discourage information requests. According to the provision, documents were to be furnished without charge or at a reduced rate when release of the information was in the public interest. And the public-interest standard was to be construed liberally by the agencies.

The January 7 memo from the Department of Justice attempted to override Congressional intent by placing an onerous burden of persuasion upon the requester. In essence, the Administration sought to discourage people from seeking information by charging exorbitant fees.

All of these actions on the part of the Reagan Administration add up to a frontal assault on the FOIA, the proven mechanism for open government. Fortunately, Congress and many public interest groups are resisting these efforts with some success. The FOIA bill now before the Senate Judiciary Committee does not

contain any of the provisions enumerated above. It does, however, still contain an offending exemption for technical data subject to export controls and restrictions on the use of FOIA by felons and foreigners which the ACLU is actively lobbying against.

As for the fee waiver issue, Rep. Glenn English, chairman of the House Government Operations Subcommittee, has spoken out vigorously against it. He sent a letter to all agency heads in which he accused the Department of Justice memo of being "biased" and warned that, "Those who unreasonably deny fee waivers when the furnishing of information can be considered as primarily benefiting the general public can expect to be invited to explain their decisions at future hearings."

THE AGENTS IDENTITIES PROTECTION ACT

ITEM: "I am willing to take risks with regard to all of the [constitutional] protections we have set up I don't think on a continuum we are going to be able to have both an ongoing intelligence capability and a totality of civil rights protection."--Senator Richard Lugar (R-Ind).

Senator Lugar was commenting, with surprising candor, on the controversy surrounding the passage by Congress of the Agents Identities Protection Act, signed into law by President Reagan on June 29, 1982.

Condemned by Professor Philip Kurland of the University of Chicago Law School as "the clearest violation of the First Amendment attempted by Congress in this era," the Act criminalizes the publication of "any information that identifies an individual as a covert agent" of the CIA or FBI--even if the information is derived entirely from public sources.

The Agents Identities Protection Act, which originated under the Carter Administration but has Reagan's blessing could intimidate an investigative reporter who writes an article about agents who participate in the CIA's destabilization of Nicaragua, or any other journalist or editor who makes a difficult decision to publish lawfully obtained information about intelligence agencies. Although the legislative history of the Act states that it is not intended to apply to investigative reporting, the express language is very broad. The statute does not require a prosecutor to show that a reporter intended to impair foreign intelligence activities by publishing an expose, but only that he had "reason to believe" that identifying an agent would do so. A warning by the CIA or even general knowledge of the CIA's sensitivity about the subject of an article, may be enough to constitute the required "reason to believe."

Since the Act's passage several reporters have published covert agents' names in the context of a news story, but no prosecutions have yet been initiated by the Administration. Perhaps it is reluctant to use a law which represents such a blatantly unconstitutional form of censorship. But if any person faces government prosecution for publishing names of agents, the ACLU stands ready and willing to offer its assistance.

EXECUTIVE ORDER ON CLASSIFICATION

ITEM: "This is an order that only a bureaucrat could write. It was drafted by security bureaucrats, who think only of how to keep everything secret, and legal bureaucrats, who think only of how to get away with filing fewer affidavits."
--Senator David Durenberger (R.-Minn.)

Senator Durenberger's acerbic comment was prompted by President Reagan's Executive Order on Classification, issued on April 2, 1982. The order, which was drafted by "a committee composed of representatives of the intelligence community" without congressional or public input, introduces major changes in the classification process.

Each successive administration over the past thirty years has issued orders making government information more, not less, available to the public. This trend toward openness culminated in 1978 when President Carter issued an order requiring government officials to consider the public's right to know before classifying information (the "balancing test"). The Carter order also instructed officials to use the lowest level of secrecy clearance when in doubt and to classify information only on the basis of "identifiable" potential damage to national security.

Under Reagan, this trend has been abruptly and unmistakably reversed. The main features of the Executive Order on Classification are:

1. It is no longer required that some identifiable potential harm to national security be demonstrated before information can be classified.
2. The "balancing test" has been eliminated so that the public's right to know need no longer be considered.
3. When in doubt officials are now required to classify material at the highest, not the lowest, possible level of secrecy.

4. Officials are mandated to classify anything which is classifiable, rather than use their discretion as under previous orders.

5. A new category of information which may be classified is added, viz. a "confidential source" which, for the first time, permits classification of domestic sources.

6. The prohibition against restoring classified status to already declassified information has been replaced by a provision specifically authorizing reclassification.

This last change can lead to rather bizarre results. Last year the Administration attempted to retrieve some previously released information from author V. James Bamford. The material included documents about secret electronic surveillance carried out by the National Security Council (NSA) and the CIA against well known antiwar activists in the 1970s. It was released to Bamford pursuant to an FOIA request made in 1979.

In early 1982 the Department of Justice claimed the information had been released "in error" and demanded that it be returned. Bamford, who used the documents in his book on the NSA, refused. Bamford's book was published, and so far no action has been taken against him.

Although the executive order has been in effect since April, 1982, a bill is currently under consideration by the Senate Judiciary Committee which would amend the Freedom of Information Act in two important respects, thereby softening the order's impact. The bill would require that before a request for information could be denied for national security reasons, the agency would have to (1) demonstrate some identifiable harm to national security which would result from the disclosure, and (2) balance that harm against the public's right to know. The ACLU is actively supporting this bill.

EXPORT CONTROLS AND SCIENTIFIC RESEARCH

ITEM: "People didn't know what to do. Rather than take a chance of violating some regulation, they decided not to present their papers."--Participant, 26th Annual Symposium of Photo-Optical Instrumentation Engineers.

This bewildered comment came after the Defense Department abruptly blocked the presentation of 100 technical papers just before they were to be delivered at the international symposium of photo-optical engineers in San Diego in August, 1982. The meeting of 2,700 technical experts was disrupted when Pentagon reviewers, who examined those papers which reported on work supported by Department of Defense contracts, concluded that some of them contained information that required a license under the International Traffic in Arms Regulations before they could be delivered to an international conference.

Some months earlier, in February, 1982, Admiral Bobby Inman sent shock waves through the academic and scientific research communities by issuing an ultimatum: Unless researchers on projects involving possible military applications agreed to submit their writings to the government for prepublication clearance, then the need to stem the "hemorrhage" of U.S. technology to the Communist bloc nations "could well cause the federal government to overreact" to the detriment of academic and scientific freedom.

The so-called "technology transfer" from West to East has become a major preoccupation of the Reagan Administration. In a misplaced attempt to prevent other countries from benefiting from U.S. technological advances the Administration has cracked down on free scientific inquiry by applying export controls (the Arms Export Control Act and the Export Administration Act) to teaching and research activities conducted by American universities and scientists. It has acted to restrict publication of unclassified research, limit discourse in the classroom, and

curtail exchanges of information and participation at conferences involving foreign students and visitors.

The programs of study of foreign students are now routinely monitored by the government. In 1981, for example, the State Department sent a letter to all universities hosting visiting Chinese scholars. Professors supervising the work of these students in computer science and satellite communications were warned that access to design, construction or maintenance data relevant to individual items of computer hardware or the design of microelectronics was prohibited. The professors were further informed that the State Department, "should be advised prior to any visit to any industrial or research facility" by such a student. No distinction was made between classified and unclassified material.

The universities have been rebelling against blatant government control. Stanford University, for example, refused to honor restrictions imposed by the State Department on a proposed visit by a Soviet robot expert, who would have been exposed only to unclassified research. The Department later backed down.

The Administration's efforts to restrict and censor the communication of unclassified scientific information is a serious threat to academic freedom and scientific inquiry. And according to a study carried by the National Academy of Sciences, open scientific communication and exchanges actually play a "very small part" in the leakage of American technology to the Soviet Union and pose no threat to our national security.

The Export Administration Act expires in September 1983. During congressional consideration of the act's renewal, the ACLU has lobbied for an amendment stating that unclassified scientific information is protected by the First Amendment and cannot be subject to restrictions under any export control scheme. Both the House Foreign Affairs Committee and the Senate Banking Committee have adopted policy amendments to this effect.

NATIONAL SECURITY DECISION DIRECTIVE

ITEM: "I'm up to my keister with leaks!"
--President Ronald Reagan.

On March 11, 1983, President Reagan issued a National Security Decision Directive which attempts to plug up the "leaks" with a vengeance. Without any congressional input or public debate, and without producing any evidence that leaks by federal employees had actually compromised national security in any way, the President signed an order which amounts to a lifetime gag order on hundreds of thousands of government employees. Essentially, the order makes applicable to all federal employees secrecy obligations which were previously only applicable to employees of the CIA and other secret intelligence services.

The order mandates that any federal employee with access to classified data must sign a secrecy agreement as a condition of employment and submit to a polygraph test if asked to do so by federal agents investigating leaks. Furthermore, those employees who have access to "Sensitive Compartmental Information" (SCI) must submit all future writings, even after leaving government service, for pre-publication review. This provision applies to every senior official in the Departments of State and Defense, all members of the National Security Council staff, many senior White House officials and all senior military and foreign service offices. It is estimated that there are about 100,000 people in government today with access to SCI.

If the pre-publication review requirement extends to all employees with access to classified information (which indeed it might, since agency heads have the discretion to include that requirement in the nondisclosure agreements they use), the covered employees will number in the hundreds of thousands.

Anyone covered by the censorship system will be subject to its rules for the rest of his or her life. All writings will have to be submitted for clearance, even if the author believes

no sensitive information is included. What sorts of writings must be reviewed? Everything from memoirs to op-ed pieces to fiction. If this program had been in effect in the past:

- the speeches and writings of Richard Allen, Alexander Haig, and Eugene Rostow would now be subject to censorship by their successors;
- political candidates such as Walter Mondale would have to clear political speeches and position papers with the White House;
- the memoirs of Henry Kissinger, Zbigniew Brzezinski, Hamilton Jordan and Jimmy Carter would be subject to censorship by their successors;
- columns by Jody Powell, Patricia Derien, Elmo Zumwalt and others would be subject to review with time delays that would make it almost impossible for them to function as columnists;
- testimony by Paul Warnke, Melvin Laird, or David Jones would have to be cleared making timely presentation to congressional committees difficult;
- reporters such as Leslie Gelb and Richard Burt would have to submit many of their articles for clearances;
- professors such as Anthony Lake and Roger Hilsman would have to clear lectures which they prepare in advance;
- consultants, investment bankers and lawyers such as Cyrus Vance, Brent Scowcroft, Richard Holbrooke and David Aaron could not submit reports to their clients before they were cleared.

It is now becoming clear that those responsible for drafting this Draconian gag order had no idea what would be involved in its implementation. Even the CIA, with a centralized system, clears manuscripts at an outrageously slow pace. How will the State Department, Defense Department, White House, National Security Council, Justice Department and other agencies deal with the staggering load which is sure to be generated by current and past employees year after year without hiring an army of censors?

Thus far congressional reaction to the order has been largely negative. Hearings have been held before the House Judiciary and Civil Service Committees. The ACLU, along with other civil liberties and press organizations, testified in opposition to the order, and pressed for congressional oversight.

II. POLITICAL SURVEILLANCE

Invoking the all too familiar catchwords "national security" and "terrorism," the Reagan Administration has turned back the clock on all the reforms made in the political intelligence field. In the post-Watergate era, when the nation was still reeling from revelations of widespread spying, infiltration and manipulation of American groups and individuals by the FBI and CIA, some restrictions, which were protective of civil liberties, were placed on those agencies. President Reagan wasted little time upon taking office in weakening those few protections.

FBI DOMESTIC SECURITY GUIDELINES

ITEM: "The guidelines permit the launching of a full investigation based on 'advocacy' alone. The Supreme Court has made it clear that mere advocacy is not enough to warrant prosecution, yet the FBI wants to investigate speech."--Rep. Don Edwards (D-Cal.), Chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights.

On March 7, 1983, Attorney General William French Smith announced the promulgation of new Domestic Security Guidelines for the FBI. These guidelines superseded those announced in 1976 by then Attorney General Edward Levi. The Levi guidelines were issued in the wake of disclosures that the FBI had engaged in widespread and indiscriminate surveillance and infiltration of civil rights, antiwar, feminist, socialist and communist organizations in the 1960s and 1970s. While not exactly a model of respect for individual rights, the Levi guidelines did at least, for the first time, impose some important and helpful limitations on the activities of FBI agents. Despite the fact that the FBI has persistently defended the Levi guidelines against

all critics, the Reagan Administration did not believe they went far enough in protecting the state against the threat of insurrection.

The most creditable contribution which the Levi guidelines made to civil liberties was the principle that the FBI could investigate domestic security threats only pursuant to a "criminal standard," not a vague hunch or suspicion. The infiltration of domestic organizations, a technique the FBI used so effectively and abusively during the 1960s and 1970s, could not be undertaken except "on the basis of specific and articulable facts giving reason to believe that an individual or a group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law"

This restriction gave a measure of protection to groups and individuals who had unpopular ideas but whose activities were constitutionally protected.

The new Smith guidelines on their face would be a significant step backward. First, they appear to authorize the FBI to open full-scale investigations, complete with such intrusive techniques as infiltration, against groups and individuals based solely on whether they "advocate criminal activity." Thus, a Nuclear Freeze Organizing Committee, whose activities consisted of collecting signatures on a petition, but whose rhetoric spoke of blocking the MX missile "by any and all means, even if we have to blockade defense installations" might be subject to FBI infiltration.

The second unsavory aspect of the new guidelines is that they would permit the FBI to use informants and infiltrate groups in "inquiries" when agents may be acting on unsubstantiated allegations. The Levi guidelines prohibited the use of such intrusive techniques in mere inquiries. They could only be used in the course of full-scale investigations which met the "criminal standard."

Finally, the new guidelines could allow the FBI to collect "publically available information" on individuals or groups who are not even the subjects of an investigation. While it sounds innocent, this provision's chilling effect is obvious enough if one lets one's imagination run free. It could lead to a vast dossier system on American citizens who are doing nothing more than exercising their rights to free speech and association.

After an aggressive lobbying campaign mounted by the ACLU and other civil liberties groups, the Department of Justice recently issued several clarifications which made the guidelines more acceptable:

1. Advocacy will be investigated only when the crime being advocated is a "credible threat" of harm or an apparent intent to commit a crime and only if criminal standards are met.

2. Public information collection must be limited to persons or groups which meet criminal investigative standards;

3. Infiltration will be conducted only in "compelling circumstances" and only with high level approval.

The ACLU is pressing to have these clarifications written into the new guidelines themselves. The House Judiciary Committee has voted to reinstate the Levi guidelines until the Department of Justice has made the appropriate changes in the new guidelines. As of early July, the bill had not reached the House floor.

EXECUTIVE ORDER ON INTELLIGENCE ACTIVITIES

ITEM: "Presidents should refrain from directing the CIA to perform what are essentially internal security tasks. The CIA should resist any efforts, whatever their origin, to involve it again in such improper activities."--Recommendation of the Rockefeller Commission on CIA activities Within the United States, 1975.

President Gerald Ford established the Rockefeller Commission

in the wake of the startling revelation that in the early 1970s the CIA had launched its "operation CHAOS" in which it collected files on 13,000 antiwar activists and indexed 300,000 names in a fruitless effort to link domestic dissenters with foreign espionage. As a result of the Rockefeller Commission's recommendations, in 1976 President Ford issued the first Executive Order on the CIA. (The National Security Act of 1947, which created the CIA, stated, "the Agency shall have no police, subpoena, law enforcement powers or internal security functions.")

Curiously, one of the members of the Rockefeller Commission, who joined in its unanimous recommendation, was "political commentator and former California Governor" Ronald Reagan.

Five years later, on December 8, 1981, President Reagan signed his new Executive Order on Intelligence Activities which, for the first time, authorized the CIA to conduct covert activity inside the U.S. The Order contains the following frightening provisions:

1. It authorizes the CIA to conduct undefined covert activities within the U.S. as long as such activities are not "intended" to influence "the political process, public opinion, policies or the media."

2. It authorizes the CIA to infiltrate U.S. organizations and influence those organizations composed primarily of aliens and believed to be acting on behalf of a foreign power.

3. It authorizes the CIA to conduct general surveillance of anyone inside the U.S. who may be in possession of "significant foreign intelligence," such as journalists or academics or business-people returning from a trip abroad.

4. It authorizes the CIA to conduct physical surveillance of U.S. citizens and corporations abroad and to monitor them for foreign intelligence, without having to first demonstrate that such individuals or corporations are working for a foreign power.

At a Presidential news conference following the announce-

ment of the order, a journalist asked for an example of how the CIA might use its new domestic authority. A senior official responded that the CIA could use its authority to help secretly persuade an international organization in the U.S. to raise and act upon an issue of American concern, such as the presence of Soviet troops in Afghanistan. This incredible hypothetical, which was delivered so breezily by a senior official of this Administration, demonstrates all too clearly the threat which the Executive Order on Intelligence Activities poses to our democratic institutions.

Earlier drafts of the executive order, which were leaked to the press (there was no official disclosure by the Administration, nor an opportunity for real public debate), met such vigorous opposition from the ACLU and other civil liberties groups and members of Congress, that a number of its worst provisions were dropped from the final order. An earlier draft would have permitted the President to authorize the CIA to conduct mail openings, burglaries, wiretaps and electronic surveillance against residents of the U.S. without a court order, and would have authorized the CIA to investigate persons in the U.S. for unauthorized disclosures of secret information. Although the Administration removed those provisions from the final draft, the ACLU is far from satisfied. In testimony given before the House Judiciary Committee's Subcommittee on Civil and Constitutional Rights, the ACLU stated:

"The Executive Order on Intelligence Activities signed by President Reagan on December 8 represents a grave threat to civil liberties. Against an overwhelming record of civil liberties abuses by the CIA, FBI and NSA and other intelligence agencies, exhaustively documented by responsible committees of both the House and the Senate, President Reagan's order represents an exercise in Orwellian doublespeak. While the Order asserts that its "procedures shall protect constitutional and other legal rights," the procedures in E.O. 12333 authorize a wide-ranging assault on civil liberties."

III. CLOSING THE BORDERS

The Administration's fear of open debate and the free flow of ideas is nowhere more transparent than in its attempts to close off America's borders to things foreign. Through the Administration's xenophobic eyes, films, books and foreign scholars have become a threat to the "national interest." By keeping the American people in isolation, little debate will accompany controversial foreign policy decisions.

LICENSING OF CUBAN PERIODICALS

ITEM: "In order for you to import the Cuban publications currently under detention by U.S. Customs Service, it will be necessary for you to obtain a specific import license from this Office."--July 10, 1981 letter from Secretary of the Treasury to subscribers.

In May of 1981, after nearly twenty years of an uninterrupted flow from Cuba of written materials, including newspapers, magazines and scholarly journals, the U.S. government, without warning, seized thousands of publications sent from Cuba to residents of the U.S.

The government claimed it was acting under the authority of regulations issued pursuant to the Trading With the Enemy Act, which, since 1963, have required a license to import goods from Cuba. However the regulations had never been enforced against periodicals before.

The regulations required a license applicant to inform the Office of Foreign Assets Control of his or her name and address, the nature of the publication, the cost and purpose of importation, and "the extent of interest of every person, including the applicant, involved or interested in the transaction." Willful

violation of the regulations could result in a \$10,000 fine and a ten year prison term! Of the thousands of American residents who receive Cuban periodicals, the vast majority were unwilling to compromise their First Amendment right to receive information by applying for an import license and the ACLU and other organizations received hundreds of protests and requests for assistance. The licensing requirement constituted a form of government surveillance over what people wished to read and learn about.

Since the importation of Cuban periodicals benefited Cuba financially only to a miniscule degree (and in any event, even free subscriptions which many Americans receive required a license), this act by the Reagan Administration could only have had an ideological basis. It was another attempt to dam the flow of politically undesirable information into the United States. Rather than permit free and unfettered inquiry, the government wants to spoonfeed only information it thinks is palatable to the citizenry.

In May, 1981, the ACLU and several other organizations filed a suit in the District of Massachusetts (the impounded periodicals were being warehoused in Boston) on behalf of more than 100 magazines, scholars, elected officials, journalists, ministers, organizations and individuals, challenging the regulation as violative of the First Amendment. In January, 1982, as a result of the lawsuit, the U.S. Treasury Department agreed to release the thousands of Cuban newspapers and magazines it had impounded, and promised to issue new regulations permitting the importation of publications from not just Cuba, but Vietnam, Cambodia and North Korea as well. The new regulations were issued, and finally the suit was dismissed when the government agreed to destroy all lists of Cuban periodical recipients which had been compiled during the impoundment.

CUBA TRAVEL BAN

ITEM: "I have been interested for some time in going to Cuba for purposes of a winter vacation and to see the country, its people and its culture. I have previously visited Jamaica and Mexico for similar reasons. In March, 1982, I decided to make a trip to Cuba for the above purposes in December, 1982, together with my children and several friends I have had to cancel the decision."
 --Affidavit of Robert C. Howard,
 plaintiff in Wald v. Regan.

After five years of unfettered travel to Cuba by American citizens, the U.S. Treasury Department promulgated new regulations in April, 1982, which prohibited American tourists from paying for "transportation related" expenses "ordinarily incident to travel within Cuba for goods for personal consumption there." In other words, the Reagan Administration banned business and tourist travel to Cuba.

The government doggedly insisted that the regulations were intended not to infringe upon the right to travel, but rather to deny Cuba the foreign currency generated by such travel.

But the facts gave lie to the government's claim. Unaffected by the regulations were foreign-based subsidiaries of American corporations which in 1980 did \$376 million worth of business with Cuba as compared to the paltry \$8 million per year spent by American tourists. Also exempt from the regulations were people with close relatives in Cuba (more than 60 percent of pre-existing travel) and those traveling for "the purpose of gathering news, making news or documentary films, or engaging in professional research, or for similar activities."

The public statements emanating from the government made the regulations sound like a blanket ban on travel, amounting

to a public relations campaign by the Reagan Administration to discourage Americans from even contemplating a trip to Cuba. Indeed, Robert C. Howard, the plaintiff quoted above and himself an attorney, cancelled his scheduled trip because, as he explained, "I am left in considerable uncertainty concerning travel to Cuba as to the purposes that might be regarded as valid and the purposes that might subject me to some form of adverse action by the government."

The new regulations represented an end-run around legislation enacted by Congress in 1978, which drastically reduced the executive branch's power to impose geographical restrictions on travel. Congress had withdrawn that authority after President Carter abrogated all restrictions on travel to Cuba, noting that it "applauded" the president's policy but sought to enact it into law to protect the "freedom of travel" principle from hostile administrations. The Reagan Administration's regulations would have rendered that 1978 law meaningless.

On June 17, 1982, the ACLU along with the Center for Constitutional Rights and the National Emergency Civil Liberties Committee sued the U.S. Treasury Department on behalf of individuals who desired to travel to Cuba and groups which organized tours to that country. The federal district court in Boston denied a preliminary injunction, but on May 16, 1983 the First Circuit Court of Appeals issued a strong decision reversing the lower court and ordering the issuance of an injunction against the travel ban. The government unsuccessfully sought a rehearing and, as of early July, was seeking a stay of the appeals court's decision and Supreme Court review.

FOREIGN AGENTS REGISTRATION ACT

ITEM: "I don't understand what they're doing because I thought part of your Constitution was freedom of speech."--Dr. Helen Caldicott, president of Physicians for Social Responsibility.

The above confusion was expressed by Dr. Caldicott, a pediatrician, when she learned that an Academy Award-winning film produced by the National Film Board of Canada, which consists largely of a speech she had delivered, had been classified as "political propaganda" by the U.S. Department of Justice. In January, 1983, "If You Love This Planet," about the medical effects of nuclear war, along with two other Canadian films about acid rain were found to constitute political propaganda under a provision of the Foreign Agents Registration Act.

This finding by the Justice Department requires the National Film Board to label the films with a statement indicating that the film board is registered with the Department of Justice as a foreign agent and that registration does not indicate approval of the films by the U.S. government. For each showing of the films, the film board is required to submit to the government the names of the theaters and organizations showing the film and the number of people in attendance.

A Justice Department spokesperson claimed the department's Foreign Agent Registration Unit had made the rulings on the basis of "common sense." But the act is worded so broadly that "common sense" simply ends up reflecting the particular political tendencies of the administration in power. And Reagan's hostility towards the nuclear freeze movement and the concerns of environmentalists is no secret. Although the films were not actually banned, the labelling and disclosure requirements of the act will undoubtedly discourage many people from attending showings of the films.

Furthermore, the derogatory classification of the films as "political propaganda" denigrates the aesthetic, artistic and educational value of the films. Rep. Jim Leach (R.-Iowa) stated the problem eloquently:

"It may be too extreme to label this act of censorship a harbinger of McCarthyism, but it sends a chilling message to those Americans deeply concerned about environmental issues in general and about the ultimate environmental issue--the survival of the planet."

On March 9, 1983, the ACLU and the New York State Attorney General filed a suit in federal court against the Department of Justice. The suit was filed on behalf of the films' distributor, a movie theater, several environmental groups, a library association and the State of New York, which was planning to show the films as part of a public education campaign about the growing dangers of acid rain in that state.

Arguing that the Justice Department's action violated the First Amendment, the complaint asks the Court for an order "enjoining defendants from stigmatizing the films in question as political propaganda and from enforcing in connection with the films any provision of the Foreign Agents Registration Act against any plaintiff or the National Film Board of Canada." In a stipulation, the government later conceded that the plaintiffs, who are not foreign agents, can cut off the "foreign agent" label before showing the films.

DENIAL OF VISAS

ITEM: "This is the dammedest thing I've ever heard. I'm beginning to believe that the Reagan Administration thinks it cannot survive criticism or free discussion of important issues."--Rep. Fortney H. Stark, Jr. (D-Ca.)

Rep. "Pete" Stark was expressing his outrage at the State Department's refusal, on March 3, 1983, to grant a visa to Hortensia Busse de Allende, widow of the slain Chilean President. Mrs. Allende had been invited to visit California for two weeks in March by the Northern California Ecumenical Council, the Catholic Archdiocese of San Francisco and Stanford University. She was to speak at a celebration of International Women's Day, meet with Chilean exiles, visit several universities and meet with San Francisco Mayor Dianne Feinstein and the Archbishop. It was not her first journey to the U.S.

One day before her expected arrival, Mrs. Allende's American sponsors were informed by the State Department that her visa application had been denied. Why? "Because her entry to make various public appearances and speeches has been determined to be prejudicial to U.S. interests because she is a highly placed official in the World Peace Council, and the Peace Council is affiliated with the Soviet Union, both ideologically and financially." And the authority for denying Mrs. Allende's visa? The infamous Walter-McCarran Act, an unappetizing left-over from the 1950s.

The fact that Mrs. Allende denies the State Department's allegations about her political affiliations is irrelevant. The important point is that the provisions of the Act have become a weapon in the hands of Reagan's State Department against foreign visitors with views opposed to this Administration's. And the ultimate loser is the American public which, once again, is denied the opportunity to learn from and debate with diverse individuals from other countries.

Mrs. Allende is neither the first nor the last foreigner to be denied entrance into the U.S. On June 7, 1983, it was learned that the State Department would bar a visit by Bernadette Devlin McAlisky, an Irish nationalist and former member of British Parliament who has been making visits to the U.S. twice a year for the last ten years. Other victims include:

--Rev. Ian Paisley, Protestant leader from Northern Ireland;

--Owen Carron, I.R.A. leader;

--Trevor Monroe, Jamaican Marxist scholar;

--Julio Garcia Espinosa, Deputy Cultural Minister of Cuba;

--Several Cuban philosophers;

--Approximately 320 delegates from Japan, Australia, Africa, Canada and Europe seeking to attend the United Nations special session on disarmament in June, 1982.

The Reagan Administration's use of the Walter-McCarran Act is a paradigmatic illustration of its fear that an informed citizenry is a threat to its reign. By barring visitors, the Administration hopes to shut out views it does not want Americans to hear.

Free Speech, 1984: The Rise of Government Controls on Information, Debate and Association was written by Loren Siegel, special assistant to ACLU Executive Director Ira Glasser, with the assistance of the following ACLU staff members: Morton Halperin, director of the Center for National Security Studies; John Shattuck, director of the national legislative office; Burt Neuborne, legal director; Jerry Berman, legislative counsel; and Charles Sims, staff counsel.

American Civil Liberties Union
132 West 43rd Street
New York, NY 10036

ACLU National Legislative Office
600 Pennsylvania Avenue, SE
Washington, DC 20003

Center for National Security Studies
(a project of the ACLU and the Fund for Peace)
122 Maryland Avenue, NE
Washington, DC 20002

Volume 1 Number 1 1984

GOVERNMENT INFORMATION QUARTERLY

**An International Journal of Resources,
Services, Policies, and Practices**

© JAI PRESS INC.
Greenwich, Connecticut London, England

Shrouding the Endless Frontier—Scientific Communication and National Security: Considerations for a Policy Balance Sheet

HAROLD C. RELYEA

Various normal and essential scientific communication activities, including unclassified research dissemination, publication, and exchanges in the open classroom and among scholars, have been limited recently by the Federal government through more vigorous enforcement and stringent application of existing national security controls. These actions are prompted by a growing anxiety about the acquisition of American science and technology by the Soviet Union and its Warsaw Pact allies. Such controls, however, may have a restrictive effect not only on scientific communication, but also on scientific achievement and advancement in the United States. Recognizing this danger, certain countervailing ideas are presented and discussed here as points of balance both to justifications for these recent limitations and to arguments favoring even broader government authority to constrain scientific communication for reasons of national security.

During the past few years, various government actions and statements by officials have reflected a growing anxiety about the transfer of American science and technology to the Soviet Union and its Warsaw Pact allies. Consequently, not only is more vigorous enforcement and stringent application of existing control authority being pursued to curtail this flow, but also new national security powers are being sought to thwart Communist bloc acquisition of our scientific information and technology having a potential for conveying a military or strategic advantage. These efforts, however, may result in a restriction of both scientific communication and scientific achievement in the United States.

Although American scientists are willing to concede that such transfers have occurred, their objections to increased government control of scientific communication should not imply that they underestimate the external dangers facing the United States, are unmindful of the need for limited official secrecy or national security safeguards, or are unaware of the potential military applications of their research and discoveries. Indeed, in taking issue with new national security limits on scientific communication, American scientists

appear to be neither politically naive about nor unappreciative of the position of their country in the continuously tense international arena. Certainly they are disturbed about the effect of such restrictions on the scientific process. Ideally, all scientific findings, conclusions, and interpretations should be publicly and generally available, open to criticism as well as improvement, and, if necessary, rejection. The vague nature of the controls being advocated by officials also is troubling. Not the least of their worries, moreover, is the pragmatic effect of new national security restrictions on scientific communication. The strength and safety of the nation will not be maintained or improved if scientific and technological progress and innovation are inhibited as a result of limitations on the dissemination of scientific information.¹ This point was well stated in the now famous report on a program for postwar scientific research which Dr. Vannevar Bush submitted to the President in 1945:

Basically there is no reason to believe that scientists of other countries will not in time re-discover everything we now know. A sounder foundation for our national security rests in a broad dissemination of scientific knowledge upon which further advances can be more readily made than in a policy of restriction which would impede our further advances in the hope that our potential enemies will not catch up with us.²

Indeed, national security results from achievement in science, not from concealment.³ And "science" and "national security" are not necessarily antagonistic to one another. In the past, scientists and government leaders have demonstrated a broad appreciation of the national security concept, including not only military applications and preparations, but also economic, cultural, and psychological considerations. In its most meaningful context, national security is not defined by Soviet military capability alone.

THE BALANCE SHEET CONCEPT

Some years ago, in analyzing the tension between national security and individual freedom, the late Harold D. Lasswell concluded "that American security measures should be the outcome of a comprehensive process of balancing the costs and benefits of all policies in the foreign and domestic fields." A national security determination, he wrote, "... is properly a policy judgment rather than an expert opinion." Many complex considerations must be assessed. "Judgments of security," counseled Lasswell, "are balance sheets of our present and prospective position as a nation under all thinkable conditions and policies."⁴

The balance sheet on increased national security control of scientific communication is under formulation. The issue, it may be argued, was opened for consideration by recent government actions, assertions, and policy recommendations. Moreover, the development of such a balance sheet seemingly is prompted by current efforts to rewrite the International Traffic in Arms Regulations⁵ and by the necessity to renew the automatically expiring Export Administration Act.⁶ Both of these authorities have been used more stringently of late to limit scientific communication.

The formulation of a balance sheet on national security restriction of scientific communication, as some may recall, is not unprecedented. Although his portrayal has a very contemporary character, the late Lloyd V. Berkner was describing the situation as it was three decades ago when he wrote that "all the important ideas of science have military implications and, under our present policies, must therefore fall inevitably under the cloak

of military secrecy." Dr. Berkner, and many other scientists, were very distressed about this state of affairs. "Since more and more of our scientific activity is coming within the purview of secrecy," he observed, "the need for appraisal of the effects of secrecy on our scientific stature and progress, and therefore on our national security, becomes of increasing importance."⁷ After identifying and discussing these effects,⁸ he then offered certain considerations for attaining "the best balance of technological secrecy as weighed against free information."⁹

At present, the Federal departments and agencies clearly may exert restrictions on the communication or dissemination of scientific research and knowledge produced by, for, or on behalf of the government. Such controls, of course, must be exercised in accordance with prevailing law regarding, for example, security classification, contracting authority, and statutorily mandated or required confidentiality. Generally, the government cannot prevent scientists unaffiliated with it or working without its financial support from communicating their research findings or knowledge unless, for example, they have produced Restricted Data as defined in the Atomic Energy Act,¹⁰ sought a patent for an invention deemed to be subject to a secrecy order,¹¹ or engaged in pursuits governed by export licensing requirements.¹² Space limitations preclude a review here of current national security authority for controlling scientific communication or the significant policy concepts pertinent to its application. However, these important elements have been considered in the larger overview from which this article derives.¹³

BEGINNING THE BALANCE SHEET

Various normal and essential scientific communication activities, including unclassified research dissemination, publication, and exchanges in the open classroom and among scholars, have been limited recently through more vigorous enforcement and more stringent application of existing national security controls. Dr. Berkner's ideas are recounted as points of balance both to justifications for these restrictions and to arguments favoring even broader government authority to constrain scientific communication for reasons of national security. They are discussed here, together with other pertinent considerations, in the contemporary context. This discussion does not presume to be systematic or exhaustive.¹⁴ These ideas are not necessarily organized in any particular priority. Finally, these are not absolute laws or postulates, but general premises and, as such, are mindful of exceptions and allowances.

The communication of basic scientific research findings and knowledge should not be subject to national security restriction, except perhaps in times of declared war. "Basic research," we are reminded, "is performed without thought of practical ends, . . . results in general knowledge. . . ." and "provides the means of answering a large number of important practical problems, though it may not give a complete specific answer to any one of them." Moreover, basic research "provides scientific capital, . . . creates the fund from which the practical applications of knowledge must be drawn," and "is the pace-maker of technological progress."¹⁵ Admittedly, the distinction between basic and applied research is difficult to make in some areas of science. Nevertheless, this judgment can be made in many cases, and should be pursued in other more difficult ones if there is to be adherence to the principle enunciated in some pertinent policy instruments that basic

research findings and knowledge shall not, for the most part, be subject to national security controls.

In July 1970, a report of the Defense Science Board Task Force on Secrecy gave support to this consideration, saying "the types of scientific and technical information that most deserve [security] classification lie in those phases close to the design and production, having to do with detailed drawings and special techniques of manufacture," and added "that most of the force of attention in classifying technical information should be directed to these phases rather than to research and exploratory development."¹⁶

The idea received policy expression in July 1978, in the Carter Administration order on security classification (E.O. 12065), and was continued by a provision of the succeeding Reagan Administration directive (E.O. 12356) which states: "Basic scientific research information not clearly related to the national security may not be classified."¹⁷

In advocating the automatic inclusion of information release terms in all Department of Defense research contracts, the recent report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements offered the following important caveat: "The Department of Defense is assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research."¹⁸ In March 1982, Acting Deputy Under Secretary of Defense George Millburn repeated this sentence in his prepared statement before two subcommittees of the House Committee on Science and Technology holding a joint hearing on the impact of national security considerations on science and technology.¹⁹ In his testimony before these same two panels, Admiral Bobby Inman, who was then Deputy Director of the C.I.A., said he had "never presumed that draconian [control] measures against the basic research side were either warranted or likely to occur."²⁰ In general, there appear to be strong indications that very little restriction of the communication of basic scientific information is warranted or planned, whether that information is produced for, by, or on behalf of the Federal Government or independently generated.

Government applications of national security restrictions to the communication of scientific research findings and knowledge should be for narrowly defined policy purposes and in accordance with specific criteria. "Freedom of communication among scientists," it has been noted, "is essential for scientific progress, and for the critical validation or invalidation of scientific findings."²¹ In the United States, scientific communication enjoys protection under the First Amendment.²² However, neither the functional need nor the civil right of scientists to communicate freely is absolute.²³ Certain particular qualifications and exceptions have been acknowledged in the past. But in this same vein, attempts to limit the dissemination of scientific research findings or knowledge should be for narrowly defined policy purposes and in accordance with specific criteria. Certainly there have been indications from within Congress which have been supportive of this point of view. For example, a 1973 House committee report on security classification policy criticized the Nixon Administration's new order (E.O. 11652) prescribing procedures for creating official secrets because of its use of such overly broad and undefined terms of policy purpose as "national security" and "foreign relations."²⁴ A more recent House committee report reprobated the classification criteria of E.O. 12356, the operative directive. During the past thirty years, succeeding presidential executive orders have narrowed the bases and discretion for assigning official secrecy to agency records. E.O. 12356 reverses this trend in a variety of ways.²⁵ The House report took

issue with the elimination of the "identifiable" damage standard for applying security classification and viewed new classification categories as overbroad, of uncertain need, and "not qualified or defined."²⁶

In 1980, a House committee report making recommendations regarding legislative reconsideration of the Invention Secrecy Act urged, among other suggestions, that Congress "Make the necessary findings and declaration of public policy that would justify the exercise of invention secrecy powers in peacetime." In addition, the report sought to "Change the basis for issuance of a secrecy order from the opinion of an agency head that disclosure might or would be 'detrimental to the national security,' to a more demonstrable standard of damage to the national defense."²⁷ All of these ideas are exemplary of the conditions contemplated by the major premise concerning narrowly defined policy purposes and specific criteria.

Primary policy and procedures concerning government application of national security restrictions to the communication of scientific research findings and knowledge should be established through the legislative process. In his study of national security and individual freedom, Dr. Lasswell makes the important comment that, because all security policies entail risk, "the public interest calls for the calculation of risk by a procedure that balances each policy against every policy and arrives at a judgment to which many minds have contributed." By using "a procedure that takes conflicting views into account and subjects them to the discipline of debate and exposure to available knowledge," the public interest can be protected and public confidence can be gained or vindicated in the wisdom of a national security policy outcome.²⁸

The Constitution vests all legislative power in Congress and prescribes the manner in which statutory laws shall be created. Through this process, Congress has established the arrangements—principally with the enactment of the Administrative Procedure Act of 1946, as amended²⁹—whereby department and agency regulations are issued and take effect. Only minimal publication requirements have been established for other executive directives,³⁰ but Congress has been counseled to extend and expand this obligation.³¹ Federal courts, on occasion, have struck down Executive Branch regulations and directives and invalidated actions taken pursuant to them; similarly, Congress, in exercising its legislative powers in an area specifically entrusted to it, has repealed agency regulations and presidential orders. However, the legislature may not divest the President of a constitutional function by legislation. As a result, there are areas of shared power. Exercising general executive authority (Article II, Section 1, Clause 1) and pursuing his responsibilities as Commander in Chief (Article II, Section 2, Clause 1), the President may prescribe policy and procedures for the protection of department and agency records for reasons of national security. Congress, relying upon its mandate to provide for the common defense (Article I, Section 8, Clause 1), to "make rules for the government and regulation of the land and naval forces" (Article I, Section 8, Clause 14), and to "make all laws which shall be necessary and proper for carrying into execution the foregoing powers" (Article I, Section 8, Clause 18) also seemingly may legislate on this subject.³² Thus, during the past few years, varying suggestions have been made from within Congress that a statutorily-based security classification system be pursued.³³

Recently, a House committee suggested that, even though a presidential executive order on security classification policy and procedure may be developed and issued without being subject to the public notice and comment requirements of the Administrative Pro-

cedure Act,³⁴ both the government and the public would be better served by adherence to the spirit of that provision. The panel recommended that future revisions of classification rules be announced publicly, that they be circulated publicly for sixty days to permit public comment, and that they "be provided to the Congress with sufficient time to permit interested congressional committees to consider the proposals, to hold hearings, and to prepare comments."³⁵

Since the conclusion of World War II, Congress has enacted various national security-based restrictions bearing upon scientific communication, and committees in both Houses have developed expertise regarding such law. The congressional forum appears to offer the best opportunity for the realization of Dr. Lasswell's proposed national security policymaking procedure. Also, as a Senate special study committee suggested not long ago in another context, administrative discretion in the execution of statutes regulating scientific communication for reasons of national security should be reduced to a minimum and guided by an instructive legislative history. Termination dates, reporting requirements, and accountability procedures were strongly suggested for legislation bearing upon fundamental civil liberties. Provision also might be made to "give Congress some type of veto over Executive branch rules and regulations judged to be inconsistent with the legislative intent of the authorizing statute."³⁶

All of these ideas are illustrative of the intent underlying the major premise regarding the establishment, through the legislative process, of primary policy and procedures concerning government application of national security restrictions to the communication of scientific research findings and knowledge.

Government application of national security restrictions to the communication of scientific research findings and knowledge, as a matter of policy, should be subject to administrative review and, in the case of privately developed information, court challenge. In the event the communication of scientific research findings or knowledge is restricted for reasons of national security, clear procedures should exist, preferably in statutory law, to permit a reconsideration of the limiting action on a de novo basis by an appropriate government official or, in the case of privately generated information, ultimately by a court to determine if the material in question warrants continued protection in whole or in part.

At the present time, E.O. 12356 provides a mandatory review procedure whereby a contractor or grantee may request that a classified work product be reviewed for possible declassification.³⁷ This arrangement, however, was designed for the general public to make declassification requests and makes no allowance for a contractor or grantee to know the details of the classification action or to enter into a discussion with government officials regarding it.

The recent report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements does not appear to make any allowance for a hierarchical appeal of initial decisions by Department of Defense officials prohibiting the dissemination of scientific information produced under departmental contract. However, peer review mechanisms discussed elsewhere in the report may include some such appellate procedure when they are fully developed.³⁸

The Invention Secrecy Act allows a private individual to appeal the imposition of a secrecy order to the Secretary of Commerce.³⁹ Although no such formal procedure exists for a private person found to be in possession of independently developed scientific

research findings or knowledge constituting Restricted Data as defined in the Atomic Energy Act, the individual in question, nevertheless, may petition the Department of Energy to remove the information from the protected category.⁴⁰ An injunction against the communication or continued possession of independently generated scientific research findings or knowledge alleged to be Restricted Data may be challenged in court.⁴¹

Clear administrative and judicial procedures should be available whenever the government applies official secrecy or communication restrictions, for reasons of national security, to scientific information. Current awareness of the importance of such arrangements would seem to be evident from the criticism recently expressed by the Department of Justice concerning the failure of proposed International Traffic in Arms Regulations "to provide prompt judicial review of State Department decisions barring disclosure" of certain technical data.⁴²

Government application of national security restrictions to the communication of scientific research and knowledge should not embrace the entirety of large undertakings, only core ideas requiring protection. This consideration is directed at two practical aspects of information protection. Large-scale projects involve many people and, in time, leaks will occur regarding aspects of the undertaking. The Manhattan Project is often cited as an example of a highly successful large-scale secret enterprise, yet there reportedly were "over 1,500 cases in which classified Project information was transmitted to unauthorized persons."⁴³

In addition, in a large-scale secret endeavor of a scientific nature, perspectives can become blurred so that support systems and knowledge related to the project, otherwise open within the scientific professions and literature, can become unnecessarily classified or restricted for reasons of national security. Both this point and the previous one were addressed in a 1956 report by a special study committee to the Secretary of Defense. It recommended that the government "(c)ease attempts to do the impossible and stop classifying information which cannot be held secret." By way of explanation, the report indicated it was referring to "information which cannot be withheld because it inevitably is known to too many people... the physical appearance and general performance data of new weapons when they have become widely known," and also "compiled data composed of unclassified items and information which is already public, where official confirmation would not be of substantial value to a potential enemy, even though it will require additional machinery to keep track of what information has been publicly revealed."⁴⁴

The number of officially secret projects involving scientific research and knowledge should be sharply limited. In more elementary terms, there are important reasons for carefully controlling the amount and duration of national security restrictions on the communication of scientific information. One obvious consideration was offered long ago by the prestigious Commission on Government Security:

... that unnecessary restrictions upon the dissemination of scientific and technological information may in the long run actually be detrimental to the national security. Positive contributions to the national security through scientific and technological advancement must not be lost as the result of an overzealous effort to classify.⁴⁵

Two other thoughts are pertinent here. Security arrangements cost money. Their efficient and economical use also suggest that information no longer in need of official protection should be declassified or removed from government control as soon as possible. Also, there is the integrity of the classification or protection system itself to take into account. Justice Potter Stewart poignantly commented on this consideration over a decade ago in his concurring opinion in the *Pentagon Papers* case, when he stated:

For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.⁴⁶

In sum, the policy point under discussion here probably was stated in its simplest terms in the Carter Administration's security classification order: "Declassification of classified information shall be given emphasis comparable to that accorded classification."⁴⁷

Government application of national security restrictions to the communication of scientific research and knowledge should be made with an awareness of the often temporary value of the information in question. A scientific discovery made today may soon be replicated or surpassed tomorrow. Government officials restricting the disclosure or communication of scientific information must be aware of this ongoing and unending process. The report of the Defense Science Board Task Force on Secrecy commented that "it is unlikely that classified information will remain secure for periods as long as five years, and it is more reasonable to assume that it will become known by others in periods as short as one year through independent discovery, clandestine disclosure, or other means."⁴⁸ Accordingly, the Task Force recommended automatic declassification scheduling, suggesting a general guideline period of "between one and five years for complete declassification," and permitting continuation of official secrecy "only if clear evidence is presented that changed circumstances make such an extension necessary."⁴⁹

Automatic termination dates are an action forcing mechanism: officials must conduct a review of protected information in order to continue restrictions on its disclosure or communication. The Invention Secrecy Act provides that a secrecy order may remain in effect for not more than one year, subject to a possible renewal.⁵⁰ By contrast, E.O. 12356, the current security classification policy directive, states:

Information shall be classified as long as required by national security considerations. When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is originally classified.⁵¹

Specifically required termination dates militate against the possibility of particular information remaining under continued official secrecy or communications restrictions after actual conditions no longer warrant such protection.

The number of persons given security clearance to examine scientific information maintained under official secrecy should be kept to a minimum. This consideration is premised on at least three expectations arising from ideas discussed earlier: the quantity of scientific research findings and knowledge placed under security classification will be

small, will contain little or no basic research information, and will be subject to automatic declassification procedures. Three practical thoughts underlie this proposition. Security clearance costs would be cut.³² Official secrets would be better protected because fewer individuals would have access to them, thereby reducing the possibilities of accidental disclosure or leaks. Some government scientists now somewhat restrained by security obligations consequently might more freely make valuable contributions to their profession and to society. With regard to this particular point, Dr. Berkner has commented:

... the maintenance of secrecy over large areas of technical information condition the scientist to miss the conception of militarily valuable ideas. Although responsible men resist such conditioning, the resulting frustrations inevitably reduce his creative effectiveness.³³

His remark seems to suggest that scientists, granted relief from the closed environment produced by security requirements and official secrecy, might apply their talents more effectively to a variety of national problems, including the country's defense situation.

An underlying principle of any policy permitting the government to apply national security restrictions to the communication of scientific research findings or knowledge should be to maintain the security of scientific progress. It is through such progress that the United States strengthens its economy, knowledge as a people, and educational and defense capabilities. Unfettered communication is a vital feature of scientific progress—all findings ideally should be publicly and generally available, and open to criticism, verification, improvement, and, if necessary, rejection. The consequences of limitations were well appreciated by the Defense Science Board Task Force on University Responsiveness to National Security Requirements and by Acting Under Secretary of Defense George Millburn when they both indicated that, if the Department of Defense "attempts to regulate the flow of scientific information in the scientific community, it could jeopardize the strength and vitality of the very community it is seeking to revitalize for the sake of national defense."³⁴

Similarly, momentary changes in our relationships with other countries may prompt some officials to seek increased protection of certain scientific information for reasons of national security. A Department of Defense study committee warned against such actions many years ago when it recommended avoiding "changing the scope of classified information to reflect temporary changes in emphasis in our foreign policy."³⁵

Scientific discovery, however, does not occur in a vacuum, unaffected by a society's values and needs. Once publicized, a scientific finding is available for anyone to use; it can be utilized in diverse ways, with consequences that may be good or bad, or commonly a complicated mixture of both. When particular scientific research findings or knowledge clearly convey a military advantage or contribute to new or improved implements of war, then the pathway is open to government protection of that information or restriction of its communication for reasons of national security. However, in preparing the balance sheet for such policy, the considerations discussed here should be included.

Widespread government application of national security restrictions to the communication of scientific research findings or knowledge are incompatible with the public policy function of a democracy. Discussing this consideration in terms reminiscent of Lasswell's words, Dr. Berkner wrote that "sound policy results from the careful ex-

amination of facts by people of a nation in light of their diverse training and interests. Continuing, he stated:

Secrecy prevents the discussion necessary to such examination, and compartmentalization prevents proper evaluation even by trained scientists. The press and other public media are the sources of the background intelligence that most influences our policy-makers and military leaders. No adequate substitute can be found in internal intelligence because information unevaluated by public debate lacks the convincing quality that results from public review.³⁶

There is another principle which is relevant to this consideration. The citizenry of a democracy must have access to information in order that they may perform their civic duties. Over a century and a half ago, James Madison stated the point in the following eloquent and memorable terms:

A popular Government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors must arm themselves with the power which knowledge gives.³⁷

At the outset of the American struggle for nationhood, the Declaration of Independence, consistent with Eighteenth Century suspicion of the state, reflected the Enlightenment assumption that neither society nor government is organic or natural to human existence. In the view of the English philosopher John Locke, whose ideas were quite familiar to the Founding Fathers, individuals contract with each other to conduct social intercourse, and subsequently establish a governing institution to protect pre-societal or "natural" rights as well as to facilitate social affairs. Implied in this arrangement is the right to withdraw from the contract when government does not fulfill its responsibilities.

In this regard, the Declaration, after postulating that governments derive "their just powers from the consent of the governed," recognizes that the state can become destructive of the rights of the citizenry. But, because there is popular "consent" to, but not "submission" to, the government exercising certain powers, such consent or support can be withdrawn when the state assumes non-delegated responsibilities, abuses its authority, or corrupts itself in the exercise of power. In order to judge the propriety of government intentions or actions, the citizenry must have information about the activities and operations of the state. In brief, the people must be watchful of their government in order to preserve popular rule.

Later, with the ratification of the Constitution, this concept of an informed citizenry received further expression in First Amendment guarantees of freedom to discuss public business, a privilege previously reserved for members of the legislature; freedom of the press, to inform the people and assist them in maintaining their watchful vigil over the state; and freedom "to petition the Government for a redress of grievances," which could include presentations against state secrecy or seeking official information.

There is no obligation in the Constitution compelling the American populace to trust its government. Departments and agencies should be willing to disclose information responsibly, not only to enhance public knowledge of their activities and policy pronouncements, but also to cultivate a degree of trust or to dispel distrust.

Widespread government application of national security restrictions to the communication of scientific research findings and knowledge keeps the public ignorant of the

adjustments it must make in the face of technological change. Noting that "(f)ailure to make adjustments to an evolving environment has in the past led to the extinction of a species," Dr. Berkner has warned that "the desire to make such adjustment can emerge in the human species only from a sound understanding of the alternatives as they become clear from public debate, or from the ultimate disaster into which society blunders."⁵⁸ Similarly, the report of the Defense Science Board Task Force on Secrecy commented that "classification of technical information impedes its flow within our own system, and, may easily do far more harm than good by stifling critical discussion and review or by engendering frustration." The report noted the incidence of "many cases in which the declassification of technical information within our system probably had a beneficial effect and its classification has had a deleterious one. . . ."⁵⁹

The strength and safety of the United States, in both the domestic and international contexts, depends, in no small part, on the ability of its citizenry to adjust to technological change. Continuous vigilance must be exercised to prevent governmental secrecy in the interest of national security from being used so frequently or becoming so pervasive that it conceals technological changes so that an unsuspecting public necessarily must adjust to them in desperation, if it can do so at all.

Widespread government application of national security restrictions to information about national capabilities in science and technology may lead an enemy to underestimate our power and encourage irresponsible adventures leading to war. This consideration seemingly assumes that government officials do not leak secret technological information of military or national security significance. Of course, some do. The motives for these anonymous, informal, and unauthorized disclosures are many and serious cold war one-upmanship figures among them. The process is one of targeted communication: selected secret technological data is passed to a trusted journalist who publicizes it in a conspicuous exclusive story which is readily obtained by foreign intelligence services.

The same objective—making the strength of the United States better known to its international foes—might be realized in a more legitimate manner by reducing, as deemed appropriate, the amount of technological information under national security control. Some decrease in information security administrative costs probably would result. The credibility of government secrecy or restriction for the technological information remaining under national security protection seemingly would be increased. And additional benefits might derive from scientists' evaluations, interpretations, clarifications, and applications of such heretofore safeguarded technological information.

OVERVIEW

Almost two centuries ago, James Madison made the following observation to his friend, Thomas Jefferson: "Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger, real or pretended, from abroad. . . ."⁶⁰ Today, the military capabilities of the Soviet Union and its Warsaw Pact allies constitute a real threat to the continued existence of the United States. But the national security of the United States cannot be understood in terms of the military capabilities of the Communist bloc alone. Fraught with risk and ultimate dangers, national security policies must be broadly conceived and formulated in such a way that conflicting views are taken into account and subjected to the discipline of debate and exposure to available knowledge.

The preservation of cherished liberty in the United States owes much to this policymaking process. Moreover, our tradition of liberty certainly has contributed in no small part to the tremendous accomplishments of scientists in this country, accomplishments that are themselves not without national security significance. Thus, any attempt by government to restrict scientific enterprise must be thoroughly examined and subjected to the rigors and demands of that cautious and considered policymaking procedure that has served us so well in the past. A balance sheet on our present and prospective position regarding any new national security policy must be prepared, debated, and assessed with great care. And a warning from the past must once again be pondered: "... without scientific progress no amount of achievement in other directions can insure our health, prosperity, and security as a nation in the modern world."¹

ACKNOWLEDGMENT

A lengthier version of this article will appear in a book of essays on the controversy over increased national security restriction of scientific communication. The views expressed here are those of the author and are not attributable to any other source.

NOTES AND REFERENCES

1. See National Academy of Sciences, *Scientific Communication and National Security* (Washington, National Academy Press, 1982), pp. 39-48.
2. Vannevar Bush, *Science—The Endless Frontier* (Washington, National Science Foundation, 1980; originally published 1945), p. 190; Cf. *Ibid.*, p. 29.
3. National Academy of Sciences, *Scientific Communication and National Security*, p. 45.
4. Harold D. Lasswell, *National Security and Individual Freedom* (New York, McGraw-Hill, 1950), pp. 53-56.
5. See 22 C.F.R. Part 121-130 (1982); a proposed version of the regulations was published in 1980, but another draft has been under preparation for some time; see 45 F.R. 83970-83995 (December 19, 1980).
6. See 50 U.S.C. App. 2401-2420; the Export Administration Act of 1979, as amended, expired automatically on October 14, 1983, but Congress continued to consider legislation revising and renewing the statute. 50 U.S.C. App. 2419 and 97 Stat. 744.
7. Lloyd V. Berkner, "Secrecy and Scientific Progress," *Science*, 123 (May 4, 1956):783.
8. See *Ibid.*, pp. 784-785.
9. See *Ibid.*, pp. 785-786.
10. See 42 U.S.C. 2014(y), 2161-2166, 2280.
11. See 35 U.S.C. 181-188.
12. See 22 U.S.C. 2751-2794 and 50 U.S.C. App. 2401-2420 which are the primary but not exclusive authorities concerning export licensing requirements.
13. This article derives from "Shrouding the Endless Frontier—Scientific Communication and National Security: The Search for Balance," a paper prepared in 1982 for the Committee on Scientific Freedom and Responsibility of the American Association for the Advancement of Science. The author especially thanks John Edsall, Lorne Feinberg, Robert Gellman, Dorothy Nelkin, Herman Pollock, Eric Stover, and Gerald Sturges for their comments and suggestions on drafts of the paper.
14. For other ideas and considerations, see, for example, National Academy of Sciences, *Scientific Communication and National Security*, pp. 52-64.
15. Bush, *Science—The Endless Frontier*, pp. 18-19.
16. U.S. Department of Defense, Office of the Director of Defense Research and Engineering, *Report of the Defense Science Board Task Force on Secrecy* (Washington, D. C. July 1, 1970), p. 1.
17. E.O. 12356, section 1.6(b), in 47 F.R. 14877 (April 6, 1982).
18. U. S. Department of Defense, Office of the Under Secretary of Defense of Research and Engineering.

- Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements* (Washington, D. C. January 1982), p. 4-4.
19. See U. S. Congress. House. Committee on Science and Technology. *Impact of National Security Considerations on Science and Technology*. Hearings, 97th Congress, 2d Session (Washington: GPO, 1982), p. 28.
 20. *Ibid.*, p. 49.
 21. John T. Edsall. *Scientific Freedom and Responsibility* (Washington, American Association for the Advancement of Science, 1975), p. 10.
 22. See James Ferguson, "Scientific and Technological Expression: A Problem in First Amendment Theory," *Harvard Civil Rights-Civil Liberties Law Review*, 16 (Fall 1981): 519-560; also see Kenneth Kalivoda, "The Export Administration Act's Technical Data Regulations: Do They Violate the First Amendment?," *Georgia Journal of International and Comparative Law*, 11 (Fall 1981): 563-587.
 23. See Edsall, *Scientific Freedom and Responsibility*, p. 5; National Academy of Sciences, *Scientific Communication and National Security*, p. 33.
 24. See U. S. Congress. House. Committee on Government Operations. *Executive Classification of Information—Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552)*. H. Rept. 93-221, 93rd Congress, 1st Session (Washington: GPO, 1973), pp. 61-62.
 25. See Richard C. Ehlike and Harold C. Relyea. "The Reagan Administration Order on Security Classification: A Critical Assessment." *Federal Bar News & Journal*, 30 (February 1983): 91-97.
 26. See U. S. Congress. House. Committee on Government Operations. *Security Classification Policy and Executive Order 12356*. H. Rept. 97-731, 97th Congress, 2d Session (Washington: GPO, 1982), pp. 13-20.
 27. See U. S. Congress. House. Committee on Government Operations. *The Government's Classification of Private Ideas*. H. Rept. 96-1540, 96th Congress, 2d Session (Washington: GPO, 1980), p. 32.
 28. Lasswell, *National Security and Individual Freedom*, p. 56.
 29. 5 U.S.C. 551 et. seq.
 30. See 44 U.S.C. 1505.
 31. See U. S. Congress. Senate. Special Committee on National Emergencies and Delegated Emergency Powers. *National Emergencies and Delegated Emergency Powers*. S. Rept. 94-922, 94th Congress, 2d Session (Washington: GPO, 1976), p. 18.
 32. See U. S. Congress. House. Committee on Government Operations. *Security Classification Reform*. Hearings, 93rd Congress, 2d Session (Washington: GPO, 1974), pp. 289-294.
 33. See H. Rept. 93-221, *Executive Classification of Information* . . . , p. 104; U. S. Congress. House. Committee on Standards of Official Conduct. *Report and Investigation . . . Concerning Unauthorized Publication of the Report of the Select Committee on Intelligence*. H. Rept. 94-1754, 94th Congress, 2d Session (Washington: GPO, 1976), pp. 43-44; and U. S. Congress. Senate. Committee on the Judiciary. *Agency Implementation of the 1974 Amendments to the Freedom of Information Act*. Committee print, 95th Congress, 2d Session (Washington: GPO, 1980), p. 36.
 34. 5 U.S.C. 551 et. seq.
 35. H. Rept. 97-731, *Security Classification Policy and Executive Order 12356*, p. 35.
 36. See S. Rept. 94-922, *National Emergencies and Delegated Emergency Powers*, pp. 12-16; although so-called legislative veto procedures were invalidated by the Supreme Court in *Immigration and Naturalization Service v. Chadha* (S. C. No. 80-1832 June 23, 1983), alternatives are discussed in Frederick M. Kaiser, "Congressional Action to Overturn Rules: Alternatives to the 'Legislative Veto'." *Administrative Law Review*, 32 (Fall 1980): 667-711.
 37. See E. O. 12356, section 3.4, in 47 *F.R.* 14879-14880 (April 6, 1982).
 38. See *Report of the Defense Science Board Task Force on University Responsive to National Security Requirements*, pp. 4-8 and 4-9.
 39. 35 U.S.C. 181.
 40. See 42 U.S.C. 2162.
 41. See 42 U.S.C. 2280.
 42. See U. S. Congress. House. Committee on Government Operations. *The Government's Classification of Private Ideas*. Hearings, 96th Congress, 2d Session (Washington: GPO, 1981), p. 277.
 43. Anthony Cave Brown and Charles B. MacDonald, eds. *The Secret History of the Atomic Bomb* (New York, Dial Press/James Wade, 1977), p. 201.
 44. U. S. Department of Defense. *Report to the Secretary of Defense by the Committee on Classified Information*, Washington, D. C., November 8, 1956, p. 12.

45. U. S. Commission on Government Security. *Report of the Commission on Government Security* (Washington: GPO, 1957), p. 180.
46. *New York Times Company v. United States*, 403 U.S. 713 at 729 (1971).
47. E.O. 12065, section 3-301, in 43 *F.R.* 28955 (July 3, 1978); this statement does not appear in the successor order, E.O. 12356.
48. *Report of the Defense Science Board Task Force on Secrecy*, p. 1.
49. *Ibid.*, p. 2.
50. See 35 U.S.C. 181.
51. E.O. 12356, section 1.4(a), in 47 *F.R.* 14877 (April 6, 1982).
52. See, for example, U. S. General Accounting Office. *Faster Processing of DOD Personnel Security Clearances Could Avoid Millions in Losses*, Washington, D. C., September 15, 1981.
53. Berkner, "Secrecy and Scientific Progress," p. 786.
54. See *Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements*, p. 4-3; U. S. Congress. House. Committee on Science and Technology. *Impact of National Security Considerations on Science and Technology*, pp. 17, 25.
55. *Report to the Secretary of Defense by the Committee on Classified Information*, p. 13.
56. Berkner, "Secrecy and Scientific Progress," p. 786.
57. Letter to W. T. Barry, August, 4, 1822.
58. Berkner, "Secrecy and Scientific Progress," p. 786.
59. *Report of the Defense Science Board Task Force on Secrecy*, p. 9.
60. Letter to Thomas Jefferson, May 13, 1798.
61. Bush, *Science—The Endless Frontier*, p. 11.

Index page 3
Volume 225, No. 21
Copyright © 1984 by The
Boston Globe
Printed in the U.S.A.
Subscription Dept.
110 South Street
Boston, MA 02111
Tel: 617-552-2222

Boston Sunday Globe

The weather
Sunday: Some sun, 20
Monday: Some sun, 30:
Details page 39
\$1.00

SUNDAY, JANUARY 22, 1984

US tightening access to information

First of three articles
by Ross Gelbman
Globe Staff

The Reagan Administration, while denying it is pursuing any formal policy, has moved systematically over the last three years to restrict or cut off access to a wide range of traditionally public information. The restrictions, unprecedented in peacetime, cover material ranging from unclassified scientific papers to information about the operation of government agencies to the writings of senior officials.

As a result, a growing number of bureaucrats, scientists, historians, journal-

ists, government contractors, unions and public interest groups are running into newly erected barriers to gathering and disseminating information.

The Administration justifies many of its specific actions on national security grounds. It claims that the nation's security depends on stemming leaks of classified information and cutting down on the flow of technological and scientific information to the Soviet Union.

But many people affected by the new restrictions charge the Administration's actions threaten academic freedom, violate constitutional guarantees of free speech and freedom from self-incrimination and

create an atmosphere of fear and intimidation among scholars, scientists and bureaucrats.

Some fear that ultimately the Administration's restrictions on information may impair the ability of society to engage in informed, timely debate about critical public policy questions.

Virtually all the restrictions have been accomplished by the executive branch — the White House, the Justice Department, the Pentagon and the National Security Council — without the approval of Congress. They include:

INFORMATION, Page 20

Reagan putting new curbs on information

INFORMATION

Continued from Page 1

Imposing lifetime censorship and the threat of random lie detector tests on about 130,000 bureaucrats and government contractors.

Rewriting the rules governing classification of documents to permit more information to be kept secret.

Permitting agencies to avoid scrutiny by obstructing the flow of previously available information under the Freedom of Information Act.

Attempting, on at least nine occasions, to suppress publication or presentation of unclassified scientific papers.

Requesting university officials to conduct covert surveillance of foreign visitors and to limit their activities.

As the White House or cabinet-level officials has responded to charges that the Administration is pursuing a conscious policy of secrecy.

Several members of Congress, in fact, have criticized the Administration for not providing such high-level matters as a former National Security Advisor William Clark or Attorney General Edwin Meese III to discuss Reagan's information policies.

White House officials, including presidential adviser Edern Meese and White House communications director David Geagan, declined repeated requests for interviews on the subject. White House counsel Fred Fielding and National Security Director Robert MacFarlane did not return telephone calls.

Through spokesmen in the Justice Dept. and other agencies, the Administration has generally defended its actions on the grounds that it needs to stop leaks of classified information. Defense and intelligence officials also have been clamping down on the flow of militarily valuable technology to the Soviet Union.

The restrictions on the Freedom of Information Act (FOIA) officials claim, are needed to counter a perception among foreign governments that the United States is engaged in criminal investigations that the government cannot protect confidential information.

But opponents charge the Administration has produced no evidence that disclosures under FOIA or leaks of confidential information by bureaucrats have endangered the national security or compromised criminal investigations.

On four occasions, congressmen have studied classified documents with one such official to see evidence of threats to national security being used to justify some of the Administration's actions. To date, the meetings have not taken place—either because of scheduling problems or disputes over ground rules.

One of the most disturbing aspects of these information restrictions is the failure of the Reagan Administration to offer a credible justification for the new policies, says Congressional critic Rep. Glenn English (D-Ola.).

"This whole business of secrecy has become pervasive," observed Dr. Robert Park, professor of physics and an official of the American Physical Society. "This is obvious. It's the first time I've ever seen it in any administration."

Harold Reyses, a specialist in American government for the Library of Congress, said there are historical precedents for some parts of the Reagan Administration's information policy, but not for its overall sweep.

President Harry Truman's guidelines for classification were as broad as Reagan's, Reyses pointed out, although they were later tightened by executive orders succeeding President. And during the early Eisenhower years, the Office of Strategic Information monitored unclassified but sensitive technical information, he said in a telephone interview.

Reyses also took issue with Reyses said, "The Reagan policies constitute an unprecedented effort to clamp down on information."

The most dramatic and highly publicized action by the Administration in this area was the banning last March of National Security Decision Directive (NSDD) #4.

Under the order, about 112,000 bureaucrats and 15,000 government contractors will have to especially sensitive information are now required, for the rest of their lives, to submit any article, book or speech they write to a review board to determine whether the piece contains sensitive information.

Acting assistant attorney general Richard K. Willard said in an interview that he drafted the order to deal with the ongoing problem of leaks of sensitive information which, he said, is a significant source of danger to the national security.

Asked to question the scope of the danger, Willard declined to respond, saying that information is itself classified. "If it's just as easy for the Soviets to read it in the newspapers, they wouldn't even have to send spies to get it."

But John Shattuck, legislative director of the American Civil Liberties Union, contended that "The directive amounts to a huge and unprecedented censorship system which is at war with the First Amendment—and for which there is virtually no justification."

Commenting on Willard's refusal to describe the problem that prompted the drafting of the directive, Shattuck added: "It's Orwellian in the extreme when the very justification for something that undermines freedom of speech is protected as secret."

Few leaks recently

Agreeing that there has been no marked increase in the number of sensitive leaks over the past few years, Willard confirmed a finding by the Government Accounting Office that there have been only 11 leaks in the past five years serious enough to require administrative action in eight agencies that handle highly classified information. Only two of the "leaks" would have been covered by NSDD#4.

One example of a "leak" was a copy of a report of the order (a) for employees who use especially sensitive information to undergo polygraph lie detector examinations—both to investigate leaks and, at random, spot-check tests.

Although they have not been accepted as evidence in court, a recent Congressional report found no evidence that polygraph results are valid and concluded that the tests run a risk of mislabeling people as deceivers.

Nevertheless, NSDD#4 states that an employee who refuses a polygraph exam may be subject to "adverse consequences."

Willard said "adverse consequences" would be most likely to apply to denying an employee access to sensitive information.

Asked why the order was necessary, when criminal laws already cover leaks of sensitive information, Willard said such cases are difficult to prosecute, since that requires disclosing sensitive information to judges and in public court records.

"He denied that an employee's refusal to undergo a lie detector test violates the 5th Amendment's right to remain silent, which guarantees the individual's right not to incriminate himself. It does not apply, he said, because an agency investigation is not the same as a criminal trial."

Mark Roth, an attorney for the American Federation of Government Employees, challenged that view. In a telephone interview, he said, "Our concern is that innocent people will have their livelihoods on the line based on admittedly unreliable tests that are not foolproof. You take the test, and you can be fired if you do. It's our feeling that it's not constitutional."

Although Willard emphasized that the order covers only a small fraction of the process with access to a minute portion of classified information, critics said that it includes high-level officials in policy-making positions.



Steven Garfinkel, director of Information Security Oversight Office of the General Services Administration, stands outside his office, heavily marked with warning signs.



Acting Assistant Attorney General Richard K. Willard defends the government's new rules on classified information.

Charles William Maynes, a former assistant secretary of State and editor of Foreign Policy magazine, told a Congressional committee that the delay inherent in the censorship process "effectively grants a standing administration censorship control over the course of debate on a large number of key public policy issues." Foreign Policy has received 61 percent of its articles from former officials "many of whom would be subject to such censorship."

Willard contended that the order would have a small delaying effect, but insisted that the CIA, which most approve such material, clears all manuscripts—including books—in an average of 15 days.

One scientist who has been involved in nuclear weapons work said the most extensive of the order would probably deter researchers from undertaking vital government-sponsored work.

Such of the American Physical Society said he conducted an informal poll of a number of senior physicists, many of whom worked on the original Manhattan Project developing the atomic bomb. The question was whether the requirement to sign a lifetime pre-publication review agreement would have affected their decision to enter government service.

"Without exception, everyone I asked said they would not have entered government service under these conditions," he said in a telephone interview.

Dr. Jonathan Knight of the American Association of University Professors, said the censorship threat could be used to harass critics. "If, as Willard claims, there is no need for a vast censorship apparatus, that is proof the order will achieve its aim simply by frightening people," he said.

It is unclear whether the Administration has begun to implement the censorship provision. Willard said nobody has been required to sign Pre-Publication Review agreements. Two senators, Charles Mathias (R-Md) and Thomas Eagleton (D-Mo), were passage of a bill last fall putting that provision of the directive on hold until April, when hearings on its implications are planned. "It would be against the law for us to require it to be signed in view of the Senate's action," Willard said.

But a scientist at a major East Coast defense planning institute said two weeks ago that most people at his institution have already been pressured to sign the pre-publication review provision.

"We were given to understand that we had to sign it or our security clearances would be in jeopardy," he said, requesting

that neither his identity nor his employer be identified.

Stressing that he has never been required to sign such agreements in the past, the scientist said, "It is an intimidating order. I'm leery about talking to you right now, even though I'm not telling you anything that's classified—just my opinion."

Broader classification rules

In addition to clamping down on those with access to highly classified material, the Administration has also moved to broaden classification rules so that more information can be kept secret.

That Executive Order, issued by the President in 1982, reversed a 30-year trend in classification rules which had progressively limited the scope of government-imposed secrecy. Specifically, the order:

Eliminated a provision barring an agency from classifying information unless it could show that "identifiable harm" to national security would result from its disclosure.

Dropped a guideline requiring that the danger of disclosure be balanced against the public right to know.

Made it easier for agencies to classify previously public material as secret after receiving a Freedom of Information request for the material.

Allowed agencies to reclassify information that had previously been declassified. Already several authors have been told they cannot allow information they gathered from open sources.

Eliminated a guideline intended to ensure that previously secret information become public after 5, 20 or 30 years depending on the material when it was no longer sensitive. The new guideline allows agencies to keep information classified as long as required by national security considerations.

A number of historical researchers US history in the early 1950s claim their work is being hampered because information which would have become public under the previous time schedule is now secret.

In an interview, Steven Garfinkel, director of the Information Security Oversight Office, responsible for overseeing all classification of documents in the government, strongly defended the changes. He said the "identifiable harm" and balancing guidelines were "a balance of interests" that they were frequently the focus of litigation to force disclosure of information—a focus, he contended, was not intended by drafters of previous classification orders.

Concerning that the classification process may be liable to abuse in some areas, Garfinkel maintained that critics are "reacting to words, not deeds." There has been, he insisted, "no change in the flow of information from the last administration to the present one."

A report being prepared for the President will show that the total amount of classification activity is up by a minimal four percent, he said. "Given the world situation, he said, that's a pretty good batting average."

Justification challenged

To critics, a fundamental objection remains that the Reagan Administration has failed to produce any evidence to justify a whole range of measures restricting the public's access to information.

Testifying before Congress last October, former Undersecretary of State George W. Ball said: "The directive (NSDD#4) can be justified only if its proponents produce compelling evidence that such an enlargement of free discourse is absolutely essential. They have not met that burden of proof. I see no evidence they ever intend to do so."

"Our current situation with the Soviet Union," he said, "is untenable, and should not lead us to justify the very Soviet methods and attitudes our leaders... deplore."

Next: Suppressing scientific papers

After getting information, writers told material had been reclassified

Magazine editor Ellis Rubenstein and authors Stephen Green and Ralph McGehee have encountered head-on a provision in the Reagan Executive Order which permits the government to reclassify a whole range of information that was previously open.

When Ellis Rubenstein, the editor of Spectrum, a magazine published by the Institute of Electrical and Electronics Engineering, received a freelance article on the Army's high-technology weapons programs, he sent the manuscript to Gen. John A. Marsh, then Secretary of the Army, to verify a quote attributed to him.

"On April 1, when I returned a call to the Army public affairs office, I was asked whether I had accepted a subsidy," Rubenstein recalled in an interview. "When I asked why, they informed me the manuscript contained classified information and should be destroyed."

"I asked what information they were referring to. They said it had a secure phrase," Rubenstein recalled in an interview. "When I asked why they identified the passage by page locations rather than reading them to me, they turned out to be three phrases in a 29-page manuscript." Rubenstein explained.

"When I told them I would check on the point of origin of the information in question, they

asked me to lock the manuscript in a safe place and call them as soon as possible."

Rubenstein subsequently told the Army that two of the phrases came from an Army publication "that is routinely made available to members of the press and public" and the third phrase was taken from testimony by the then-Army Chief of Staff Lt. General Donald R. Keith in public session of Congress.

On April 5, the Army spokesman called Rubenstein and conceded the first two phrases were not, in fact, classified but added, "Lt. General Keith's testimony remains classified and should be deleted from the manuscript."

Rubenstein asked how the Army could classify open testimony in Congress.

"The spokesman explained that sometimes unclassified data, put together into a particular context, can be classified," Rubenstein said, which is greater than his parts, in such cases, government can reclassify unclassified material," Rubenstein related.

What was especially ironic, in Rubenstein's view, was that two of the phrases he wanted deleted were descriptions of Soviet rockets—information that originated in the Soviet Union.

About two years ago, Stephen Green, writing a book on tensions between the US and Israel, requested and received 47 pages of documents from the National Archives.

Several months later, Green received a call from Edwin Thompson, director of Records Administration at the Archives, asking him to return the 47 pages so they could be copied and recorded.

In a telephone interview, Green, who is based in Montpelier, Vt., said he waited about five weeks for the material to be returned. It was not.

When he contacted the aid of the American Civil Liberties Union, an Archives official told him the "initial reviewer had failed to identify... items that might not have been classified." Shortly thereafter, the material was returned to Green—with 11 pages withheld and seven other pages substantially deleted.

It was only when the ACLU threatened to sue the Archives on Green's behalf that the material returned to him. Green said he subsequently learned the Archives had been asked to reclassify the material by the Air Force and the State Dept.

Last March, former CIA agent Ralph W. McGehee published a



Ralph McGehee, an author and former CIA official, says Central Intelligence Agency officials tried to conceal a book he was writing about the agency.

book strongly critical of CIA policies that, he claimed, resulted in the transmission of misleading intelligence designed to support the position of US policy makers.

In an appendix, McGehee described his three-year effort to get his manuscript approved by CIA censors.

One objection of the CIA's Publication Review Board (PRB) involved a section in which McGehee described early training and psychological testing of CIA recruits. When McGehee pointed out that the same information had appeared in books by such pro-CIA authors as William Colby, Ray Clive and Allen Dulles, the censor countered that, "The reviewer said it had made a mistake

earlier when it had approved that information."

McGehee replied, "That's tough... it can't reclassify information."

The censor's response, said McGehee, was, "We're operating under a new order," referring to the Reagan order permitting reclassification. McGehee was able to publish the information by pointing out that the Reagan order was at that time still in draft form and had not yet officially taken effect.

In a telephone interview, McGehee said the publication review process at the CIA was used almost exclusively to pressure him to delete information that was not sensitive but was embarrassing to the agency.

In November, testifying before a House committee on President Reagan's pre-publication review directive, McGehee said:

"From my experience, I conclude that the CIA, reacting as its bureaucracy, uses publication review and spurious claims of national security to prevent the American people from learning of its illegal and embarrassing operations."

"I am sure that the American people deserve to know the truth about our democratic process. The CIA's efforts demonstrate what we can expect from other agencies. Even the mere authority under President Reagan's Executive Order."

- ROSS GELSPAN

Sci-Tech

- Programming computers to help doctors in their diagnoses.
- The cholesterol conundrum.

56 pages

The Boston Globe

The weather

Tonight: Cloudy, in 20s
Tomorrow: Warmer, rain likely
Details, Page 27
25 cents

Vol. 225, No. 23-c, 1984, Globe Newspaper Co.

MONDAY, JANUARY 23, 1984

Telephone 929-2000

Classified
Circulation
929-1500
929-7272

When US aids the work of scientists

Following is the second in a three-part series on the efforts of the Reagan Administration to place tighter controls on public access to government information and to some types of scientific communication.

By Ross Gelbspan
Globe Staff

When scientists arrived in San Diego to attend a conference of the Society of Photo-Optical Instrumentation Engineers in mid-September 1982, many of them were summoned to a room to meet with Department of Defense personnel.

The officers asked two questions: "Was your work sponsored by a DoD agency? Have you secured clearance for your papers?"

That was enough. The scientists withdrew about 150 papers from the conference.

Prof. Hajime Sakai, of UMass-Amherst's Department of Physics and Astronomy, withdrew a non-classified paper he had prepared on measuring atmospheric emissions. He said he objected but felt he had no choice because the research was done under a Defense Department contract.

Today, he is angry over the incident, calling it a government effort to censor scientific exchanges of information.

"We thought that there was no restriction in our contract on publication or presentation of the work if it has scientific merit," he said in a telephone interview. "The reason we objected is that academic freedom is at stake."

A Pentagon official involved in INFORMATION, Page 20

When scientists' work is US-sponsored

IS INFORMATION

Continued from Page 1
The affair denied the scientist was a "general attack on the scientific community."

"We were just trying to get Defense Department contractors to live up to their obligation to clear any work before presentation," said Dr. Stephen D. Bryen, deputy assistant secretary of defense for international trade and security policy.

But Sakai, emphasizing the non-sensitive nature of the work, was persuaded. Since the San Diego conference, he said, he has been required to send one copy of his work to the Defense Department, which sponsors his work, so that officials there can advise on its use of words.

"It's not strictly censorship," he said, "but most of us know that to be, in a way, censorship. They can only advise us. But if we don't observe that advice, probably they can withhold future grants. They don't say that explicitly, but that is the implication."

Attempts to stop presentations

On at least nine occasions in the last three years, Defense Department officials have tried to prevent scientists from publishing or presenting their papers at scientific conferences. They also have denied visa applications to prevent foreign scientists from attending scientific meetings, at virtually all cases, the material in question was not classified.

No one outside the Pentagon is sure how many such interventions there have been, but the American Academy for the Advancement of Science, the leading organization of US scientists, is compiling a list of them.

Concern is growing, meanwhile, that an effort to control the free exchange of scientific information in the name of national security may eventually threaten the very vitality of American science.

The cause of those unpredictable "gaps of information" in Defense Department publications has called them, in a few among many in the Reagan Administration that the United States is "oversecreting technology" to the Soviet Union.

As one result, the Defense Department is underwriting a major effort by the US Customs Service to intercept the export of military critical technology.

It also has requested university officials to conduct covert surveillance of foreign visitors and to limit their activities.

And it has sought, through legislation, through proposed changes in the Freedom of Information Act and through expanded use of its power to classify information, to apply new controls to unclassified scientific information with potential military applications. That definition, many scientists claim, could cover almost any scientific development.

Hapazard restrictions

While virtually all scientists concede the need for secrecy in specific areas of research that could provide direct military benefits to the Soviet Union, a growing number express concern about the hapazard imposition of hapazard restrictions on scientific communications.

In November, Dr. Freda, president of the National Academy of Sciences, told the House Judiciary Committee "perhaps most disquieting from the point of view of individual US scientists is that these [international and other governmental actions to control scientific communication] have been largely disjointed, unpredictable and vague in specifying the scientific fields they are intended to cover. The result is that individual scientists are quite unclear about what obligations and sanctions, if any, might apply to her or his work."

More fundamentally, a number of scientists and university presidents contend that the government has produced no evidence to support its contention that the Soviets are gaining critical military information from open scientific literature.

Dr. Paul E. Gray, Massachusetts Institute of Technology president, has not on to be queried with top Defense officials, including Secretary Casper Weinberger, and said in an interview: "Not one of the examples I've heard of or heard about — relates to the transfer of technology through the open scientific literature. All the examples are in the area of espionage or intentional export of high-tech items to the USSR."

In the observations of the CIA, said Dr. Gray, who is supported by the former deputy director of the CIA, Adm. Bobby Ray Inman, who believes only a small percentage of the "open" scientific literature to the Soviet Union comes from universities.

Similarly, a blue-ribbon panel convened by the National Academy of Sciences found that "in comparison with other channels of technol-



PHOTO BY ART STERN

"We have an uncanny ability to advertise what we're doing. But many scientists are simply not willing to listen. What we need back from the scientific community is some real cooperation... Some journals make us out to be evil McCarthyites. Instead, what the scientists should be doing is suggesting creative solutions, helping us get the job done."

Stephen D. Bryen



GLOBE PHOTO BY BANA CORNWELL

"Not one of the examples I've heard — or heard about — relates to the transfer of technology through the open scientific literature. All the examples are due to theft, espionage or unintentional re-export..."

Dr. Paul E. Gray

ogy transfer, open scientific communications involving the research community do not present a national danger from non-structure military implications." That report is commonly referred to as the Corson Report, since the panel was headed by former Cornell University president Dale Corson.

Critics also point out that virtually no classified work is done on the campuses of American universities.

New regulations sought

However, Bryen is less sanguine.

"No one really knows how much data the Russians get from the open literature and from scientific exchanges," Bryen said of former members of defense establishments involved in research and engineering, and a more practicable and less restrictive set of guidelines.

The groups are hammering out a new set of regulations to deal with the problems of technology transfer.

The Corson Report minimized the damage from technical data. The Soviets operate with great precision," Bryen said in an interview. He added that the Soviets key their efforts to secure information to research developments in the United States.

Bryen, who has been responsible for a number of recent Pentagon efforts to have scientific papers withdrawn, said, "We have an uncanny ability to advertise what we're doing, but many scientists are simply not willing to listen. What we need back from the scientific community is some real cooperation."

Many scientists, he feels, either refuse or are unable to understand the severity of the threat posed by the Soviets to US security.

"The groups are hammering out a new set of regulations to deal with the problems of technology transfer. The Corson Report minimized the damage from technical data. The Soviets operate with great precision," Bryen said in an interview. He added that the Soviets key their efforts to secure information to research developments in the United States.

Pointing out that about 90 percent of defense programs are not classified, Bryen said the military is less likely to decide what information to release and more likely to project and to decide how to carry out that protection.

One means, he said, involves listening across to scientific literature.

He held up a copy of Defense Electronics magazine, open to an article on radiation-resistant microchips. Affixed to the magazine was a note from one of Bryen's staff members, asking why the ma-



BACK LEFT PHOTO

terial in the article was not classified.

"The problem is that no one is deciding whether it's right or wrong to publish material like this. Smart people ought to sit down and decide whether it's wrong," he said.

"If there's a lot of information on the street, it's easy for the Russians to get it." When asked for ex-

amples of Soviet military gains from Western technology, however, many in the defense establishment point not to the inflating of scientific literature but to government-sponsored sales of nonmilitary technology, which the Soviets have converted to military uses.

In a speech to the Armed Forces Communications and Electronics Assn., for instance, Navy Adm.

"Perhaps most disquieting... is that these and other governmental actions to control scientific communication have been largely disjointed, unpredictable, and vague..."

Frank Press

civilian use, to repair Soviet aircraft carriers, nuclear submarines and other warships.

Members of the scientific community point out that Soviet acquisition and secrecy in most papers delivered at scientific conferences is acceptable to most high-technology companies, which don't publish their research. The publication which is of benefit to their competitors.

C. Peter Magrath, president of the University of Minnesota, argues that most scientific work done at universities has no immediate applications.

The work done at universities
Magrath's view is supported by Dr. William R. Free, chairman of the Technology Transfer Committee of the Institute of Electrical and Electronics Engineers Inc., a society with about 230,000 members worldwide, 190,000 of whom live in the United States.

In a telephone interview, Willenbrock pointed out that the level of defense and secrecy in most papers delivered at scientific conferences is acceptable to most high-technology companies, which don't publish their research. The publication which is of benefit to their competitors.

Science and technology do their best in a free society, he added. "Some people want to shut it down and throw out all foreign scientists. It's a Fortress America concept, but it is based on serious misapprehensions. The notion that all good science is done in the US, for example, is ridiculous."

MIT's Gray and others contend that the greatest casualty of government-imposed secrecy could be the continued development of science within the United States.

Computer scientist Stephen H. Unger, of Columbia University, argued that the free exchange of knowledge among scientists and engineers is a key factor in promoting progress. An integral part of the scientific process is the publication and dissemination of new ideas, discoveries and experimental results. By this means, critics may detect errors or faulty reasoning, point out possible improvements or confirm the validity of what was done...

There is no way to block the flow of information to the Soviet without... slowing its own scientific progress more than it would slow down theirs.

As an example, Gray cited work done in secret on the development of high-speed uranium centrifuges by the Atomic Energy Commission.

"The work progressed very slowly while it was classified," he said. "When it was opened up somewhat to the rest of the scientific community, it turned out that a lot of others had been working on some of the problems which had been impeding the progress of the work. A lot of time and money could have been saved by having the process open."

Robert Rosenzweig, of the American Assn. of Universities, in a telephone interview, asked rhetorically: "Why do we produce science that others want to steal?"

"It must have to do with the social system of science we've developed. And that has to do with competition of ideas. It's that which has the advantage away for libraries or short-term protection seems unwise policy."

NEXT: Restrictions on the Freedom of Information Act

ONE CASE OF PAPERS BEING WITHDRAWN

Dr. Stephen D. Bryen, deputy assistant secretary of defense for international trade and security policy, leaned back in his leather chair in his fourth-floor office at the Pentagon.

"Yes, I was involved in having the six papers withdrawn from the International Conference on Permafrost last July."

He pointed to a huge map of the world covering virtually an entire wall of his office.

"Look up there," he said, pointing to the Siberian region of the Soviet Union. "You see that? Did you know that the Russians have serious problems maintaining their military facilities in that area?"

He turned from the map.

"There were several Russians at the conference."

Bryen thumbed through a file on the conference, which was in Parkanna, Alaska.

"Look at the list of the papers we had withdrawn; they deal with the maintenance of airfields and roads on permafrost, with pipeline construction, with the performance of off-road vehicles on tundra terrain."

"Can you imagine having Defense Department-sponsored scientists working the Russians on how to maintain their airfields in Siberia?"

"Those papers came out of the Army Corps of Engineers' Cold Regions and Engineering Laboratory," he said, adding that the Defense

Department, as a sponsor of the work, had every right to order the papers not be presented at the conference.

Dr. Lloyd Brestau, technical director of the laboratory, prefers to look at the positive side: "The fact that six papers were deemed to be sensitive or classified doesn't detract from the fact that we were able to go ahead with 23 other presentations. I'm delighted that we were able to disseminate that much information."

But other scientists involved in the conference are not persuaded.

"The papers involved no classified information," said Dr. Timothy Muehlen, of the National Research Council. "We never knew any official explanation for the papers' withdrawal. The authors were quite displeased."

"It's difficult to say what security issues might have been involved," he concluded.

Said Prof. Robert D. Miller, a soil physicist at Cornell University who was on the committee that selected papers for presentation at the conference: "From what I know of those papers, the value of them to any potential adversary is quite limited. In fact, I would guess, given the USSR has been investigating the same matters for a longer time and in more places than we have."

tals to any military security is something someone would suggest to a young scientist that he join a Defense Department lab because of the fear that "arbitrary decisions may be made... the feeling that there might be capricious or invasive reactions for denying publication of something that had scientific merit and defensible security implications."

"That would be a chilling prospect for a young scientist and would damage the nation's Defense establishment in long run because of the prospect of losing the ability to attract the high quality staff they've always been able to attract."

Miller emphasized in a telephone interview that his judgment was that of a military person, but he said: "The pertinence of any de-

-ROSS GELSPAN

The Boston Globe

Business Extra

- Some views of the economic climate under Dukakis.
- A gamble for Apple.

64 pages

The weather

Tonight: Occasional rain, 30-32
 Tomorrow: Partly sunny, 40-45
 Details, Page 43
 25 cents

Vol. 225, No. 240 1984, Globe Newspaper Co.

TUESDAY, JANUARY 24, 1984

Telephone 928-2000

Information, please

Reagan directives are coming under scrutiny

This is the last in a three-part series on efforts by the Reagan Administration to restrict access to information that has traditionally been considered public.

By Ross Gelfman
 Globe Staff

"This legislation springs from one of our most essential principles: A democracy works best when the people know all the information that the security of the nation permits. No one should be able to put up curtains of secrecy

around decisions which can be recalled without injury to the public interest."

With these words President Ronald Reagan in 1980 signed into law the Federal Freedom of Information Act, passed by Congress to counter a tendency toward secrecy in government agencies in the wake of World War II and the Cold War.

Despite a consensus among most of those who use and administer the act that the law has grown

INFORMATION, Page 18

Reagan's revised information act under scrutiny



'FOIA has occasionally disrupted vital law enforcement activities and has been misused by businesses ...'

Sen. Orrin Hatch (R-Utah)

INFORMATION
Continued from Page 1

ally worked well, the Reagan Administration has made a number of changes in the way federal agencies respond to information-act requests.

Many who regularly use the act claim that those changes, along with amendments to the law being sought by the Administration, constitute a clear signal to bureaucrats to withhold information wherever feasible.

The Administration denies any such intent. Jonathan C. Rose, an assistant US attorney general, testifying before Congress last April, declared that the Administration "strongly supports the basic purpose and philosophy of the act."

Rose said the changes proposed or implemented by the Justice Department involved only a few specific "narrow problems" such as use of the act by criminals to undermine investigations, inadequate protection of proprietary commercial information and increasing costs to government for processing information-act requests.

Information-act users, however, claim that various kinds of information, freely available from government sources before 1981, have been restricted - either through new interpretations of the act or through the imposition of prohibitive fees, sometimes in situations where fees had been waived entirely in the past.

Said one veteran information-act officer at a major federal agency who declined to be identified: "The flow of information has definitely been diminished.... The Administration came in to emulate the Freedom of Information Act."

Restrictions are cited

Users of the information act cite a multitude of examples of restrictions on information that has traditionally been available, usually at no cost:

• When Jim Lyon of the Environmental Policy Institute in Washington, D.C., learned last summer that the Interior Department had produced a report documenting that strip-mine operators

had failed to pay millions of dollars in reclamation fees, he asked for a copy. Such reports had always been available in the past.

He was told to file an information-act request.

When he did, an Interior Department official told him that the agency would charge him \$500 an hour to process his request, he said.

Lyon appealed, saying the rate would be prohibitively expensive for his organization. Interior officials have yet to respond to the appeal he filed last September, citing a large backlog of appeals. "The government is very successful in keeping information from the public by changing its traditional policy of waiving fees," said Lyon. "I find it very alarming."

• Last July, Les Norrgard, chief investigator for the Better Government Assn., a public-interest group that monitors waste and fraud in government, filed an information-act request with the State Department to obtain recently completed audits of US embassies.

At the time, the association was looking into complaints by some ambassadors that they were incurring extraordinary costs in entertaining official US visitors, including junketing congressmen, business executives and other officials.

When he requested a fee waiver, Norrgard said, an information-act officer denied the request, stating, "I do not believe the information will primarily benefit the general public." Norrgard appealed the denial on Aug. 22.

In early September, United Press International produced a series of articles on an excessive entertainment expenses at several European embassies. Not long afterward, Frank M. Machak of the State Department denied the fee-waiver appeal, stating in a letter,

"There is no demonstration of heightened [public] interest in the expenditure of funds by embassies abroad." At the time the letter was received, the UPI articles had appeared in at least 30 newspapers and had been the subject of a special report on CBS radio.

"This is the first time we've had to sue on this issue," Norrgard said. "Why we're being put through this drill is very disturb-

ing."

• Last November, a Boston-area housing consultant working with a Lowell tennis organization filed an information-act request with the Department of Housing and Urban Development for a developer's financial statement. Those statements have always been available to tenant and community groups who are deciding whether or not to contract with a developer.

A HUD official refused the request, apparently as a result of a December 1982 memorandum from the HUD Washington office which states succinctly: "Until further notice, do not release any more Profit and Loss Statements under the FOIA."

• When Philip Simon of the Center for the Study of Responsive Law filed an information-act request last fall with the Occupational Safety and Health Administration for its memorandums on a report by the center which criticized OSHA, he received a copy of one memorandum. An accompanying letter told him that was all the information the agency had on file.

Several weeks later - when Simon was on the telephone with an OSHA employee reviewing the memorandum paragraph by paragraph - he realized material had been deleted from his copy of the memorandum. There was no indication on his copy that deletion had been made. Simon sued the agency three weeks ago, contending it violated the information act by failing to notify him of information that was being withheld.

• Eric Goldschmidt, a reporter for Food Chemical News, had been routinely receiving results of Agriculture Department inspections of meat packing plants.

When he asked for a similar report last year, he was told he would have to file an information-act request. When he did, Agriculture officials turned down the request saying that the inspection reports were part of an investigative file. Goldschmidt subsequently filed suit, won a summary judgment and obtained the reports.

• In May, 1982, the health and safety director of the AFL-CIO requested routine enforcement data from OSHA.

"In the past, we've always gotten this information with no problem and at no charge," said Margaret Seminario, associate director of Occupational Safety, Health and Social Security for the AFL-CIO. "But under the Reagan Administration, the agency has been quite nasty about it."

"When the agency did not respond to informal queries, the union filed an information-act request for the reports on worker fatalities.

OSHA responded by saying they did not have the information and that it would cost the union about \$70,000 for the agency to compile it.

"Ultimately," Seminario said, "we did get most of the information. In some cases we had to go through Congressional committees. In others, anonymous sources in the agency provided the material."

"It's interesting that information we were told was not available just happened to become available when Congress demanded it."

• Greg Gordon, a UPI reporter, said when he requested a sample of Medicaid claim forms from the Veterans Administration for an article on health regulations, he was told it would cost him more than \$64,000.

In a telephone interview, Gordon said he subsequently negotiated a lower fee with the agency. "It took about four months before we reached agreement and another nine months before the agency processed the request. By that time, I was on to something else and could not get to the bottom of it."

• Prof. Barton Bernstein, a historian at Stanford University, cited a change in State Department policy in which the department now charges information-act requesters for the time required to review material before deciding whether or not to disclose it.

"I can tell you I felt, in effect, barred by that decision...." Bernstein said in a telephone interview. "It's clear they're using costs to withhold information."

'Aberrant examples'

Asked about several of these examples, Kevin Jones of the Justice Department said he could not comment on individual cases with which he was not familiar.

"Obviously we don't have control over an agency's day to day administration of the FOIA. The stories you're telling me sound like aberrant examples," Jones said.

However, Jack Taylor, an investigative reporter for the Denver Post who has made extensive use of the information act, disagrees with Jones: "The changes are subtle, but there is a pervasive atmosphere emanating from the top. Because of the atmosphere of secrecy, bureaucrats have become more inclined to keep things private."

Until recently, the impact of Justice Department directives on the information act were not readily discernible, said Eric Glitzenstein, an attorney with the Ralph Nader-sponsored FOI Clearinghouse, who handles a number of suits. "But now the examples are beginning to rain down," Glitzen-



'... if important information remains beyond our grasp - we will soon lose the means to effectively criticize government.'

Sen. Patrick Leahy (D-Vt.)

stein said. "The signal to FOI officers is clear: Avoid compliance with FOI requests whenever possible. Freedom of information is being regarded in a much more hostile fashion, to be avoided at all costs."

Jones disputes such allegations, saying, "The charge has been made and, I think, irresponsibly by some. The Department of Justice is dedicated to implementing the act, to reducing backlogs, to making sure information that is public be kept public, and to make government pricing policy more uniform."

Ratch defends amendments

Added Sen. Orrin Hatch (R-Utah), who led the fight on behalf of the Justice Department's information-act amendments in the Senate: "Just as the FOI Act holds the government accountable to an informed electorate, FOIA itself must be held accountable. Since [the act was rewritten in 1974], it has at times frustrated rather than fulfilled its basic mission of insuring government efficiency and informing voters. FOIA has occasionally disrupted vital law enforcement activities and has been misused by businesses who... found it a convenient tool for obtaining confidential information about a competitor."

Despite Administration statements to the contrary, a number of people who use the information act (only about 10 percent of whom are journalists) believe the Administration's desire to restrict information has been clearly signaled to federal agencies in several ways, including:

• A memorandum in May 1981 from Attorney General William French Smith informing agency heads that the Justice Department would henceforth support in court any agency's decision to withhold information from an information-act requester.

• A package of amendments to the act proposed by the Justice Department in late 1981 to significantly expand exemptions under the act. One proposed exemption would have permitted government

agencies to withhold information submitted by companies on race and sex discrimination, dangerous drugs and environmental pollution. The proposed amendments were subsequently watered down in negotiations between Hatch and Sen. Patrick Leahy (D-Vt.), who will cosponsor a compromise package of amendments in the next session.

• In August 1982, President Ronald Reagan issued an executive order which, among other things, makes it much easier for agencies to reclassify as secret information which had been previously made public.

• In January 1983, Rose, the assistant attorney general, ordered agencies to reverse a 10-year practice of waiving fees for most requests that fall into a "public interest" category. Rose's memorandum directs agencies to apply five specific criteria in order to make their own determination of the potential value of information to the public.

Criteria is criticized

Rep. Glenn English (D-Okla.) said last year that, "These criteria invite an agency to substitute its own judgment for that of the requester. It is inappropriate to use fee waivers in this fashion."

For Leahy, who has been leading the fight in the Senate against the Administration's proposed amendments to the act, the law is "an invaluable tool for turning government accountability from a catchphrase into a reality." He said it has been used to disclose government waste and wrongdoing, expose discrimination and secure data on defective and harmful products.

In a speech last fall before the American Newspaper Publishers Assn., Leahy warned:

"If we let things drift - if important information remains beyond our grasp - we will soon lose the means effectively criticize government. If we ever lose the means for very long, we will in time find we will lose the right...."

End of series

'The signal to FOI officers is clear: Avoid compliance with FOI requests whenever possible.'

Eric Glitzenstein, attorney with FOI Clearinghouse



MS MAIN FILE COPY

The Reagan Administration Order on Security Classification: A Critical Assessment

83-1237

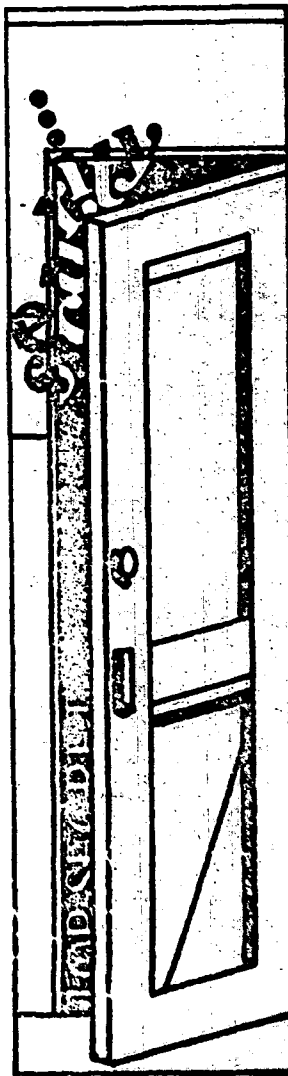
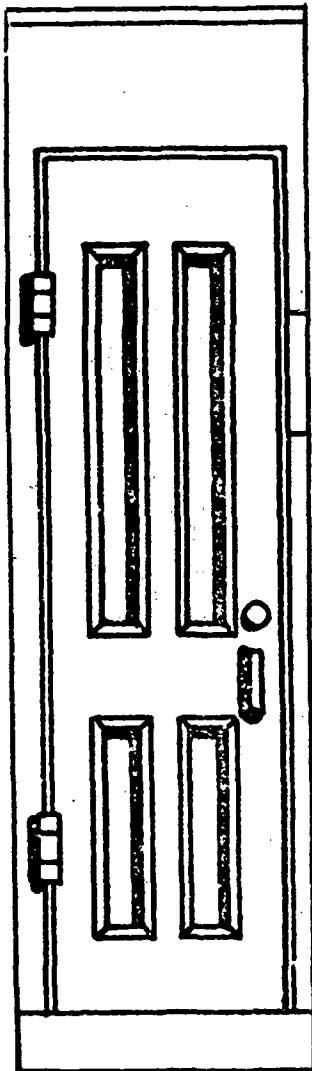
RICHARD C. EHLKE AND
HAROLD C. RELYEA

President Reagan's executive order prescribing new security classification policy and practice is the latest in a series of such directives which first appeared in 1940. During the past thirty years, succeeding presidential classification orders have narrowed the bases and discretion for assigning official secrecy to agency records. However, E.O. 12356, issued in April, clearly reverses this trend by expanding the conditions for classification, requiring the application of official secrecy whenever possible, and maintaining records under security protection in perpetuity. This assessment of the new executive order reviews the evolution of classification policy, critically examines the Reagan directive, and explores its implications for the Freedom of Information Act.

Classification evolves

During the early years of the Federal Government, the practice of assigning official records a secret status was not directly sanctioned by law. Although statutes establishing the Departments of State and War, among others, contained provisions mandating the issuance of housekeeping regulations concerning the custody, use, and preservation of their papers, more explicit authority for protecting sensitive foreign affairs documents and communiques was not conferred for over a half a century.¹ In 1857, the President was empowered "to prescribe such regulations, and make and issue such orders and instructions, not inconsistent with the Constitution or any law of the United States, in relation to the duties of all diplomatic and consular offices, the transmission of their business, . . . the safekeeping of the archives, the public property in the hands of all such officers [and] the communication of information . . . from time to time, as he may think conducive to the public interest."²

Richard C. Ehlike is a Legislative Attorney with the Congressional Research Service of the Library of Congress. Harold C. Relyea is a Specialist in American National Government with C.R.S. The views expressed in this article are solely those of the authors and are not attributable to any other source.



pn-1

Armed forces security-secrecy instructions seemingly did not appear until 1869. Initially limited to prohibiting the unauthorized photographing or sketching of forts or coastal defenses, these orders passed through a series of metamorphoses and, by the time the United States entered World War I, evolved into a fully developed information classification system with special graduated document protection markings, need-to-know access restrictions, and personnel security clearances. With the return to "normalcy," armed forces regulations governing the creation and safeguarding of official secrets were continued and soon assumed a pervasive character. By 1936, Army classification instructions seemed to embrace not only sensitive military matters, but also foreign policy material and what might be properly described as "political" data. The "Secret" designation referred to information "of such a nature that its disclosure might endanger the national security, or cause serious injury to the interests or prestige of the Nation, an individual, or any government activity, or be of great advantage to a foreign nation." Similarly, "Confidential" could be applied to material "of such a nature that its disclosure, although not endangering the national security, might be prejudicial to the interests or prestige of the Nation, an individual, or any government activity, or be of advantage to a foreign nation." Moreover, the term "Restricted" might be used in instances where information "is for official use only or of such a nature that its disclosure should be limited for reasons of administrative privacy, or should be denied the general public."

By the time of the initial years of the New Deal, armed forces security classification requirements and controls had permeated not only many civilian sectors of the Departments of War and Navy, but also some other government entities to which protected records had been transmitted. Although the creation of official secrets largely was limited to the national defense community, this authority could be exercised with broad discretion to embrace matters well beyond traditional military considerations. In addition, Army and Navy security classification regulations during World War I and into the late 1930s often made general reference to criminal law to give them force, even though the cited statutory authority seems to have been of more limited or narrow applicability than was implied by the armed forces instructions.⁴

Presidential orders

For reasons not entirely clear today, security classification policy and practice became a matter of direct presidential specification in 1940. This development probably was promoted somewhat by desires to clarify the authority of civilian personnel in the national defense community to create official secrets, to establish a broader basis for protecting military information in view

of growing global hostilities, and to better manage a discretionary power seemingly of increasing importance to the entire Executive Branch.

Relying upon a 1938 statute concerning the security of armed forces installations and equipment and "information relative thereto," Franklin Roosevelt issued the first presidential security classification directive in March, 1940. E.O. 8381 authorized the use of control labels on "all official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts or specifications which are now marked under the authority of the Secretary of War or Secretary of the Navy as 'secret,' 'confidential,' or 'restricted,' and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President." The order made no reference to penalties or to sanctions under the espionage laws in the event its provisions were violated. For the most part, E.O. 8381 paralleled armed forces regulations for marking and handling secret records, gave civilian employees of the War and Navy departments authority to classify information, and was confined largely to traditional national defense—rather than "national security"—matters. However, the legislative history of the 1938 statute, upon which the President relied to issue his order, provided no indication that Congress anticipated or expected that such a security classification arrangement would be created.⁵

During World War II, various prerogatives were exercised to protect sensitive information. In addition to the President's order and prevailing armed forces directives, the Office of War Information, in September, 1942, issued a government-wide regulation on creating and administering classified materials. Among other ad hoc arrangements, personnel cleared to work for the Manhattan Project, in committing themselves not to disclose protected information improperly, were "required to read and sign either the Espionage Act or a special secrecy agreement."⁶

Congress did not directly authorize any of these secrecy innovations during the war years. However, immediately following the end of the world hostilities, security policy for particular types of information was legislated. The Atomic Energy Act of 1946 provided protection for certain "Restricted Data" concerning "the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power." This authority was renewed in 1954 and has been extended by subsequent enactments.⁷ The National Security Act of 1947 specified that the Director of Central Intelligence "shall be responsible for protecting intelligence sources and methods from unauthorized disclosure."⁸ Later statutes supplemented this requirement.⁹ And with the adoption of the Internal Se-

curity Act of 1950, Congress reiterated its commitment to the criminal punishment of any Federal official or employee who communicates classified information without authorization.¹⁰

During this same period, security classification policy was being reconsidered at the White House. In February, 1950, President Truman issued E.O. 10104, superseding E.O. 8381, but relying upon the same 1938 statute cited for the earlier directive. This new order added a fourth "Top Secret" classification designation, making American information security categories consistent with those used by our allies. However, at the time E.O. 10104 was promulgated, plans were underway for a complete overhaul of the classification program. The result was a dramatic change in policy.

E.O. 10290 of September, 1951, introduced three sweeping innovations in security classification policy. First, the order indicated the Chief Executive was relying upon "the authority vested in me by the Constitution and statutes, and as President of the United States," rather than a specific statutory provision, in issuing the directive. Politically, such reliance upon implied constitutional powers strengthened the President's discretion to make official secrecy policy; it intertwined his responsibility as Commander-in-Chief with the obligation to "take care that the laws be faithfully executed."¹¹

Second, information was now classified in the interest of "national security," an imprecise and nebulous policy term also conveying considerable latitude for the creation of official secrets. By contrast, previous security classification executive orders had been confined to traditional military and naval or national defense matters.

Third, as a reflection of the more expansive view of information protection, the order extended classification authority to nonmilitary entities, to be exercised, presumably but not explicitly limited to, those having some role in "national security" policy.

The broad discretion to create official secrets granted by E.O. 10290 engendered widespread criticism from the public and the press. In response, President Eisenhower, shortly after his election to office, instructed Attorney General Brownell to review the order with a view of revising or rescinding it. The subsequent recommendation was for a new directive which was issued in November, 1953, as E.O. 10501. It withdrew classification authority from 28 entities, limited this discretion in 17 other units to the agency head, returned to the standard of applying secrecy in the interest of "national defense," eliminated the "Restricted" area and explicitly defined the remaining three classification categories to prevent their indiscriminate use, provided for reviews of protected records for purposes of downgrading or declassification, and clarified procedures for handling classified information to alert Federal em-

ployees to the dangers of its unauthorized disclosure.

Nevertheless, E.O. 10501 also appeared to exhibit some deficiencies. Although a prestigious national study commission indicated the tripartite classification categories were overly broad and suggested, for reasons of efficiency and economy, that the "Confidential" area be abolished, this recommendation was ignored.¹³ In 1962, the House Committee on Government Operations strongly urged "that the Defense Department establish administrative penalties for misuse of the security system" and reiterated an earlier proposal addressing "the lack of an effective procedure for appeals against abuse of the information classification system."¹⁴ A few years later, another report by this oversight panel lamented the President's reliance upon implied constitutional and statutory powers to issue E.O. 10501 and noted that its past recommendations regarding an effective appeals procedure against classification abuses and administrative penalties for overclassification of information had not been accepted.¹⁵ However, during the decade following the issuance of E.O. 10501, several clarifying memorandums and amending executive orders were promulgated to correct other deficiencies in the directive.¹⁶

Security classification policy and procedure next came under presidential review and restatement in 1971. A special interagency committee developed a draft revision of E.O. 10501 during the year and circulated it to selected departments and agencies for comment during January of 1972. After adjustments were made as a result of this process, the directive was promulgated in March as E.O. 11652.

The new order withdrew classification authority from a number of agencies, the most significant reduction occurring in the "Top Secret" category from which 31 entities were eliminated. Although the President issued E.O. 11652 "by virtue of the authority vested in me by the Constitution and statutes of the United States," the preamble included references, as well, to the Freedom of Information Act and the Federal criminal code. The order sought to clarify and tighten the basic standard for classification, but in doing so, it reintroduced the overly broad "national security" referent. Whereas the minimal basis for classifying information under E.O. 10501 was that disclosure "could be prejudicial to the defense interests of the nation," under E.O. 11652 it was that disclosure "could reasonably be expected to cause damage to the national security." Moreover, a National Security Council directive issued in May, 1972, implementing the new order indicated that "any substantial doubt" about the appropriateness of a classification designation should be resolved in favor of "the less restrictive treatment," which could mean no secrecy at all in some situations.¹⁷

The new order created general, automatic declassification schedules of six, eight, and ten years for the three categories of protected records, but provided that official secrecy could be retained for selected documents. However, the mandatory declassification review procedure established by E.O. 11652 obligated agencies, at the request of the public, to examine identified records classified for ten or more years to determine if they were any longer in need of protection or might be released. The new order also provided in general terms for administrative reprimands in the event of "(r)epeated abuse of the classification process," including the unnecessary classification or overclassification of information.

Criticism of E.O. 11652 was expressed within Congress regarding both the manner in which the order was developed and its content. A report by the House Committee on Government Operations noted that "The appropriate committees of the Congress having extensive experience and expertise in the oversight of the security classification system were not given the opportunity by the executive branch to comment on the design of the new Executive order."¹⁸

Scrutinizing the content of E.O. 11652, the Committee's report indicated that the new directive, among other shortcomings, improperly implied that the first exemption of the Freedom of Information Act should be mandatorily applied; confused the applicable authority for punishing "an alleged 'wrongful disclosure' of classified information or material described in Executive Order 11652;" failed to distinguish between important policy terms such as "national defense" and "national security" and made no attempt to meaningfully define them; restricted public access to lists of individuals having classification authority and permitted departments and agencies "to hide the identity of classifiers of specific documents;" legitimized and broadened authority "for the use of special categories of 'classification' governing access and distribution of classified information and material beyond the three specified categories;" and created "a 'special privilege' for former Presidential appointees for access to certain papers that could serve as the basis for their private profit through the sale of articles, books, memoirs to publishing houses."¹⁹ The Committee concluded its report on security classification policy and practice by strongly recommending "that legislation providing for a statutory security classification system... be considered and enacted by the Congress."²⁰ Subsequently, reports from two other congressional panels have echoed this view.²¹

By the autumn of 1977, the Carter Administration had developed an initial draft of a new executive order on security classification policy and procedure. Comments on the preliminary version of the directive were invited from both Congress and interested private organizations. In July, 1978, it was promulgated as E.O. 12065.

Although the President continued to rely upon implied constitutional and statutory powers to issue the new order, the preamble was devoid of any reference to the Freedom of Information Act, but did indicate that the general purpose of the directive was "to balance the public's interest in access to Government information with the need to protect certain national security information from disclosure." In serving this objective, E.O. 12065 narrowed the minimal basis for creating official secrets. Whereas the basic standard for classifying information under E.O. 11652 was that disclosure "could reasonably be expected to cause damage to the national security," under the new order it was that disclosure "could reasonably be expected to cause identifiable damage to the national security." The "substantial doubt" criterion for classifying records, which had appeared in the directive implementing E.O. 11652, was upgraded to the text of E.O. 12065 and provided that "If there is reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified." Moreover, the order also introduced an important new balancing test, stating: "In some cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified." When such questions arose, a high level official, specified in the order, would "determine whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure."

Other innovations in E.O. 12065 designed to restrain the application and impact of security classification included the permissive creation of official secrets, expressed in terms of an understanding that information "may not be considered for classification unless it concerns" certain sensitive areas specified in the order; a requirement that records "indicate clearly which portions are classified, with the applicable classification designation, and which portions are not classified;" a stipulation that "(b)asic scientific research information not clearly related to the national security may not be classified;" an avowal that a "product of non-governmental research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified... until and unless the government acquires a proprietary interest in the product;" a prohibition stating that classification "may not be restored to documents already declassified and released to the public;" an operative understanding that "(d)eclassification of classified information shall be given emphasis comparable to that accorded classification;" and a policy of systematic review of permanently valuable

classified records of the government when they become 20 years old to determine whether they should be declassified or continued as official secrets. E.O. 12065 also withdrew classification authority from some agencies, the most significant reductions occurring in the "Secret" and "Confidential" categories where the number of entities was decreased by approximately 50 percent.

Although informal consultations with congressional overseers identified and resolved disputes over some aspects of the draft order, these efforts did not overcome all criticism of it from this quarter. An analysis by the staff of the House Subcommittee on Government Information and Individual Rights indicated dissatisfaction with the directive's oversight and control mechanisms, characterizing them as "notably deficient in detecting and correcting abuses of the system."³³ Commenting on the new entity created within the General Services Administration to monitor compliance with the requirements of E.O. 12065, the Subcommittee staff analysis offered the following assessment: "Given GSA's lack of political or economic leverage over most agencies with classification authority, placing the Oversight Office within GSA does not seem to portend particularly vigorous enforcement of the order."³⁴

Other weaknesses in the directive identified by the Subcommittee staff analysis included "no general declassification schedule" and "no requirement that the classifier mark the document he is classifying to show which of the criteria he is relying upon."³⁵ Concern also was expressed about the possible abuse of procedures for extending classification beyond the basic six-year terminus or waiving periodic declassification reviews of permanently valuable records.³⁶

E.O. 12065 became effective in December, 1978, and it remained operative policy, without amendment, for the next three and one half years.

Policy reversal

Six months after the Reagan Administration assumed office, White House Counselor Edwin Meese acknowledged in a national press interview that "there is way too much classification." According to the President's friend and advisor, "You really should only classify something if its revelation would actually harm the national security."³⁷ A few weeks after these comments were published, an initial preliminary version of a replacement for E.O. 12065 was circulated among selected department and agency officials by the Deputy General Counsel of the C.I.A. It is doubtful that the policy disposition and procedures expressed in that draft order would have restrained the excessive security classification about which Mr. Meese had complained.

During the autumn and winter of 1981 and into the first months of the new year,

the process of refining the draft security classification order continued within the Executive Branch. On February 4, the tentative text of the directive was made available for the first time to selected congressional committees with an indication that the deadline for receiving comments about it was approximately two weeks away. In response, a February 10 letter signed by eight chairmen of committees or subcommittees of the House of Representatives protested the brief comment period, requested that the imposed deadline be extended, and declared that "No change should be made in the Executive Order without allowing for thorough review."

The Administration agreed to extend the comment deadline by a few weeks, but declined to send witnesses to mid-March hearings on the draft order scheduled by the House Subcommittee on Government Information and Individual Rights. As a consequence of this development, the chairman and two other members of the panel took the unusual step of sending a letter directly to the President asking that a spokesman be sent to testify on the draft order. Two Administration representatives, neither of whom held policymaking positions, subsequently appeared before the Subcommittee in early May, but by that time the directive had been signed by the President.³⁸

The comments and criticisms independently expressed during February and March by various members of Congress, congressional committees, and private organizations regarding the draft executive order were not without effect. Just before the President signed the directive, several changes in its text were acknowledged and credited to reviewers outside of the Executive Branch. A list of officials having original classification authority and implementing instructions for E.O. 12356 subsequently were published and the order became effective on August 1, 1982.³⁹

During the past thirty years, succeeding presidential classification directives have narrowed the bases and discretion for assigning official secrecy to Executive Branch documents and materials. E.O. 12356 appears to reverse this trend in three general ways: the protection of information is emphasized disproportionately over the public accessibility of government records; some previously valued limitations on classification criteria and discretion are eliminated; and other new broad conditions for classification are established. Indeed, there is considerable concern that the policy changes made by the executive order will prompt more frequent resort to classification and, consequently, will increase the quantity of official secrets. Such a development has evident implications not only for the public availability of information and government security costs, but also for the integrity of the classification program. Justice Stewart warned of these perils over a decade ago in his concurring opinion in the *Pentagon Papers* case:

For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.⁴⁰

Although its preamble professes that "it is essential that the public be informed concerning the activities of its Government," E.O. 12356 appears to give greater priority to the safeguarding of information against unauthorized disclosure than to maintaining an equilibrium between the government's need to protect materials and the public interest in the disclosure of records. In this regard, the new order implies that official secrecy should be applied in a mandatory manner. Indicating that information "shall be considered for classification" if it concerns certain specified broad topical categories, the order states that information within one or more of these categories "shall be classified" if "its unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security."

The "substantial doubt" standard of E.O. 12065 concerning the possible protection of information is significantly modified. Now, when there is "reasonable doubt" about the need for official secrecy, the matter is to be resolved by having the material at issue "safeguarded as if it were classified." Similarly, a question about the appropriate degree of protection is to be decided by having the record under consideration "safeguarded at the higher level of classification." Although such actions must be affirmed by an original classification authority, the operative presumption is for maximum classification, a reversal of the relevant policy positions of both E.O. 11652 and E.O. 12065.

Administration witnesses appearing before the House Subcommittee on Government Information in early May indicated that the balancing test of E.O. 12065 is an unstated but inherent aspect of classification policy under E.O. 12356. The draft version of the directive implementing the new executive order had stated: "The exercise of classification and declassification authority inherently includes the consideration of the public interest served by protection or disclosure." This provision, however, does not appear in the promulgated version of the directive.

E.O. 12356 omits and discontinues various limitations and restraints on classification criteria and discretion which had evolved from previous executive orders. It eliminates the "identifiable" qualifier from

its basic standard for classifying information, thereby returning to the minimal condition established in 1972 by E.O. 11652, that disclosure "reasonably could be expected to cause damage to the national security." In his May testimony before the House Subcommittee on Government Information, the Director of the Information Security Oversight Office indicated that classifiers will be expected to have some particular damage in mind when they apply official secrecy to a record, but it would appear that this may be a much more abstract or theoretical harm than the "identifiable" damage required by E.O. 12065.

Unlike its two immediate predecessors, E.O. 12356 establishes no basic classification time period(s) leading to automatic declassification or selective continuation of protection for a limited quantity of materials. The primary policy premise of the new order regarding the duration of official secrecy is that records "shall be classified as long as required by national security considerations." It then adds the following discretionary allowance: "When it can be determined, a specific date or event for declassification shall be set by original classification authority at the time the information is originally classified."

Other limitations and restraints on classification abandoned by E.O. 12356 include a prohibition on classifying a product of non-governmental research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access until and unless the government acquires a proprietary interest in the product; a specification that the declassification of official secrets be given emphasis comparable to that accorded classification; and a requirement that all special access programs be reviewed regularly and, with the exception of those required by treaty or international agreement, be terminated automatically every five years unless renewed in accordance with prescribed procedures. In addition, although E.O. 12065 required that all classified agency documents and papers 20 or more years old be systematically reviewed with a view to declassification, E.O. 12356 makes such efforts discretionary or optional and limits them to permanently valuable records not yet accessioned into the National Archives.

Among the new conditions introduced by E.O. 12356 broadening the applicability of official secrecy are three new classification categories pertaining to information concerning "the vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security," "cryptology," and "a confidential source." Because the first two of these areas are not defined in the order, they may be interpreted broadly to embrace any functional unit or organization of physical or intellectual property no matter how vaguely "relating to the national security" and all cryptology. The third category is defined to in-

clude both actual and potential confidential sources.

Although E.O. 12065 specifically prohibited the restoration of official secrecy to records already declassified and released to the public, E.O. 12356 reverses this policy, allowing the reclassification of "information previously declassified and disclosed if it is determined in writing that (1) the information requires protection in the interest of national security; and (2) the information may reasonably be recovered." However, two recent attempts by the government to retrieve and reclassify publicly released agency records suggest that such actions may not be very satisfying due to the adverse publicity they appear to produce and the seeming necessity of relying upon voluntary compliance to obtain the materials at issue.¹⁸ Like E.O. 12065, E.O. 12356 also permits the classification or reclassification of information after an agency has received a request for it under the F.O.I. Act, the Privacy Act, or the mandatory review provisions of the order.

With E.O. 12356, both a greater quantity and variety of information seems destined for security protection. Resort to classification is encouraged; conditions and criteria for applying classification are broadened; and discretion for imposing classification is increased. Indeed, the new order seems to be rather unmindful of the need for effective declassification arrangements. Bulging and growing files of official secrets are expensive to maintain. As the quantity and variety of classified records increases, new storage equipment must be obtained, secure facilities must be expanded, more personnel must be cleared to keep protected materials in good order, and many others must be cleared and approved to use these documents. And apart from these property and managerial costs to government, the classification policies and practices of E.O. 12356 also will exact a toll on public access to Executive Branch records.

F.O.I. Act impact

The Freedom of Information Act accepts the standards and procedures of the prevailing security classification executive order for excepting official secrets from mandatory public disclosure. The first exemption of the Act (5 U.S.C. 552(b)(1)) permits an agency to withhold information pertaining to matters that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." In this manner, Congress has indicated a willingness to defer to the President to determine the conditions by which a certain kind of sensitive information shall be assigned a protected status exempting it from disclosure under the F.O.I. Act. Therefore, a change in the prevailing executive order on security classification effectively results in a modification of the first exemption of the F.O.I. Act.

The link between the security classification executive order and the first exemption of the F.O.I. Act has been a feature of the law since its enactment in 1966. For the first seven years of its operation, the Act exempted from mandatory disclosure matters that were "specifically required by Executive order to be kept secret in the interest of national defense or foreign policy." The Supreme Court broadly interpreted this provision as a *per se* exemption for records bearing a classification stamp and held that courts were not to look behind a protective marking to determine the propriety of classification in exemption one cases.¹⁹ Congress reacted by including in its package of 1974 amendments to the Act a revised exemption one, the provision presently in the Act. The intent was to require courts, as part of their responsibility to review agency actions under the F.O.I. Act, to satisfy themselves that classification decisions were arrived at correctly, both procedurally and in conformity with the substantive criteria of the operative executive order. Although the judicial acceptance of classification decisions encouraged by Mink was rejected, Congress, mindful of the sensitivity of the information involved, admonished courts to give "substantial weight" to agency representations regarding the classification of information and the harms likely to result from its disclosure.²⁰

With rare exception, classified records have not been made public as a result of F.O.I. Act litigation.²¹ Courts seldom second-guess the classification decisions of agency officials. If agency affidavits are sufficiently detailed in describing how particular information falls within classification categories, such declarations usually are adequate for purposes of *de novo* judicial review of the agency's action. Thus, judgment on the basis of agency affidavits is warranted "if the affidavits describe the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith."²²

In camera review of documents by the court is available in exemption one cases, as well as in all F.O.I. Act cases. However, it is employed less frequently in litigation involving classified records.²³ If agency affidavits prove deficient, the agency may be given the opportunity to submit more detailed affidavits in camera or to make an oral in camera presentation.²⁴ The nature of national security information and intelligence operations also may prompt an agency to neither confirm nor deny the existence of records responsive to an F.O.I. Act request. This tactic also has been sanctioned by the courts.²⁵

In addition to the extraordinary procedures permitted in national security cases, courts also have been deferential in review-

ing agency compliance with the criteria of exemption one, namely, whether or not the information was classified in accordance with the procedures of the prevailing executive order and whether or not it falls within the substantive classification categories claimed by the agency. Courts thus have excused procedural errors when the classifiability of information otherwise has been demonstrated.¹⁰ The inherently speculative nature of predicting harm to the national security upon disclosure of particular information also has been recognized by the courts, which have noted that to demand more than a plausible demonstration that the predicted danger is a reasonable expectation would be "overstepping by a large measure the proper role of a court in national security F.O.I.A. case."¹¹

E.O. 12356 is not likely to change these basic standards of judicial review in exemption one cases. Courts will still give "substantial weight" to agency affidavits, which in most litigation will prove sufficient to enable court review of agency claims. However, to the extent that the new executive order results in more classification, less declassification, and the longer duration of classification, less information naturally will be accessible under the F.O.I. Act. In this regard, the order's expansion of the categories of classifiable information, its mandate that information falling within the categories be classified, the availability of classification, and the elimination of automatic declassification undoubtedly will make official secrecy a greater barrier to the public accessibility of government records through the F.O.I. Act. More information thus will be subject to the first exemption of the statute and effectively immune from searching judicial scrutiny of agency decisions not to disclose it.

Some elements of E.O. 12356, in addition to resulting in a greater quantity of classified information, also hold the potential to restrict even further the nature and scope of judicial review of F.O.I. Act cases involving exemption one. Two changes from the previous executive order have caused particular concern in this regard and have prompted a legislative proposal to counteract them.

As noted earlier, E.O. 12356 eliminates the balancing test contained in E.O. 12065 and also deletes the modifier "identifiable" from its basic standard for classifying information. With respect to the first of these differences, most courts have viewed an agency's application of the balancing tests to be within its discretion and reviewable, if at all, under an abuse of discretion or arbitrary or capricious standard.¹² Some cases, however, have indicated that greater judicial scrutiny of an agency's balancing decisions is appropriate.¹³ No definitive criteria have emerged, so it is difficult to assess the impact that elimination of the balancing test from the new order will have in terms of court review of exemption one claims.

The effect of the deletion of the modifier "identifiable" from the basic classification standard of E.O. 12356 also is uncertain. No court has focused on the presence of the qualifier as adding significantly to the burden on an agency to demonstrate classifiability of materials. In one case, the court noted the absence of the modifier in E.O. 11652 and its appearance in E.O. 12065, but concluded that the difference was not substantial.¹⁴ The obligation on an agency to make its case for exemption involves a process of identification and justification which would seem to make the presence of the modifier somewhat redundant. Thus, as with the elimination of the balancing test, the deletion of "identifiable" from the basic classification standard is likely to have little practical effect on F.O.I. Act litigation.¹⁵

The new order also expands the types of information which, if disclosed, presumptively will cause damage to the national security. It stipulates that "Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security." The prior executive order provided that only the disclosure of foreign government information or the identity of a confidential foreign source would be presumptively harmful. The U.S. Court of Appeals for the District of Columbia, in the only opinion elaborating on the implications of the presumption in E.O. 12065, described it as a "powerful one," involving information which was unique among all categories of information subject to classification. The court went on to hold that the plaintiff had not supplied sufficient evidence of non-damage to overcome the presumption and specifically declined to rule "when, if ever, a F.O.I.A. requester can overcome the presumption that disclosure of [confidential foreign government information] will damage our national security."¹⁶

Thus, an F.O.I. Act requester has the burden of rebutting the presumption of damage for certain types of foreign information under E.O. 12065. The expansion of the presumption to embrace "intelligence sources or methods," both foreign and non-foreign, will place that burden on more requesters as more information will be subject to the presumption. The court's leaving open the question of the ability of a requester to ever overcome the presumption may portend a significant shift in the burden of proof and scope of judicial review in such cases. The expansion of the category of presumptively harmful information in E.O. 12356 obviously would broaden the impact of that development.

In summary, probably the greatest effect E.O. 12356 will have on the F.O.I. Act will be to increase the amount of information subject to classification and to extend the duration of secrecy permitted under the order. The withholding of national security information is subject to different, more

deferential judicial review under the Act. To the extent that F.O.I. Act requesters are confronted with more assertions of exemption one as a result of the provisions of the new order, less information is likely to be released. Other changes in classification policy made by E.O. 12356, such as the elimination of the balancing test and the "identifiable" qualifier, although indicative of the desire to tighten classification standards and practices, will likely have less of a practical effect on the F.O.I. Act than the overall expanded universe of classified information likely to flow from the new order.

OVERVIEW

During the past thirty years, three Presidents have issued security classification executive orders successively narrowing the bases and discretion for assigning official secrecy to Executive Branch information and materials. E.O. 12356 clearly reverses this trend by expanding the categories of classifiable information, mandating that information falling within these categories be classified, making reclassification authority available, admonishing classifiers to err on the side of classification, and eliminating automatic declassification arrangements.

The general results of these policy changes are likely to be more classification, less declassification, and the longer duration of official secrecy. The consequences of these developments, in turn, seemingly will be much greater administrative expense to the government, less public access to agency records under the F.O.I. Act, and questionable control of private data and infringement on intellectual freedom. Ultimately, the integrity of the classification program itself may hang in the balance.

FOOTNOTES

¹⁰See *Federal Register*, v. 47, April 6, 1982, pp. 14874-14884; *Ibid.*, v. 47, April 12, 1982, p. 15557.

¹¹See 1 Stat. 28, 49, 65, 68, 553; 9 Stat. 395; 16 Stat. 163; 17 Stat. 283; and 18 Stat. 169. With the compilation of the *Revised Statutes of the United States* (1874), these separate authorities were combined in a single provision at Section 161 which was continued in various editions of the United States Code without alteration until 1958 when a single amending sentence was added (72 Stat. 547); the provision presently is located at 5 U.S.C. 301.

¹²11 Stat. 60.

¹³See Harold C. Pelyea, "The Presidency and the People's Right to Know" in Harold C. Pelyea, ed. *The Presidency and Information Policy*, New York, Center for the Study of the Presidency, 1981, pp. 9-17.

¹⁴See 52 Stat. 3.

¹⁵Anthony Cave Brown and Charles B. MacDonald, eds. *The Secret History of the Atomic Bomb*, New York, The Dial Press/James Wade, 1977, p. 201.

¹⁶See 60 Stat. 755, 766.

¹⁷See 68 Stat. 919; 940; 42 U.S.C. 2014(y), 2162; also see, for example, 94 Stat. 780, 788 and 95 Stat. 1163, 1169.

¹⁸See 61 Stat. 497; 498; 70 U.S.C. 403(d)(1).

¹⁹See, for example, 63 Stat. 208, 211; 90 U.S.C. 403g.

²⁰64 Stat. 987, 991; 50 U.S.C. 783.

"See U.S. Commission on Government Security, *Report of the Commission on Government Security*, Washington, U.S. Govt. Print. Off., 1957, pp. 174-176.

"U.S. Congress, House, Committee on Government Operations, *Safeguarding Official Information in the Interest of the Defense of the United States*, House Report No. 2456, 87th Congress, 2d Session, Washington, U.S. Govt. Print. Off., 1962, p. 13.

"U.S. Congress, House, Committee on Government Operations, *Executive Classification of Information—Security Classification Problems Involving Exemptions (b)(1) of the Freedom of Information Act* (5 U.S.C. 552), House Report No. 93-221, 93rd Congress, 1st Session, Washington, U.S. Govt. Print. Off., 1973, pp. 11, 23-26.

"See House Report No. 2456, *supra* note 13, pp. 11-12.

"See *Federal Register*, v. 37, May 19, 1972, pp. 10053-10054.

"House Report No. 93-221, *supra* note 14, 102.

"See *Ibid.*, pp. 58-71, 75-83.

"*Ibid.*, p. 104.

"See U.S. Congress, House, Committee on Standards of Official Conduct, *Report on Investigation Pursuant to H. Res. 1042 Concerning Unauthorized Publication of the Report of the Select Committee on Intelligence*, House Report No. 94-1754, 94th Congress, 2d Session, Washington, U.S. Govt. Print. Off., 1976, pp. 43-44; U.S. Congress, Senate, Committee on the Judiciary, Subcommittee on Administrative Practice and Procedure, *Agency Implementation of the 1974 Amendments to the Freedom of Information Act*, Committee Print, 95th Congress, 2d Session, Washington, U.S. Govt. Print. Off., 1980, p. 36.

"See U.S. Congress, House, Committee on Government Operations, *Security Classification Exemption to the Freedom of Information Act*, Hearings, 95th Congress, 1st Session, Washington, U.S. Govt. Print. Off., 1979, p. 95.

"*Ibid.*, p. 101.

"*Ibid.*, pp. 96-97.

"*Ibid.*, pp. 96-99.

"Meg Grossfield, "A Talk With Edwin Meese," *Washington Post*, July 7, 1981, p. A15.

"See U.S. Congress, House, Committee on Government Operations, *Executive Order on Security Classification*, Hearings 97th Congress, 2d Session, Washington, U.S. Govt. Print. Off., 1982.

"The list of officials with original classification authority appears in *Federal Register*, v. 47, May, 1982, pp. 20105-20106; the implementing directive for E.O. 12356 appears in *Ibid.*, June 25, 1982, pp. 27836-27842.

"*New York Times Company v. United States*, 403 U.S. 713, 729 (1971).

"See *Judith Miller*, "Agency Demands Docu-

ments Back," *New York Times*, March 14, 1982, p. 19; George Lardner, Jr., "Air Force Pulls Back on '53 Secret Papers," *Washington Post*, April 5, 1982, p. A5; George Lardner, Jr., "Air Force Abandons Attempt To Reclassify Old Documents," *Washington Post*, April 20, 1982, p. A2.

"*Environmental Protection Agency v. Mink*, 410 U.S. 73 (1973). The court recognized (410 U.S. at 83) Congress' power to prescribe classification procedures of its own, but noted that it instead had opted to adopt the criteria of the pertinent executive order in enacting exemption one of the F.O.I. Act.

"U.S. Congress, Senate, Committee of Conference, *Freedom of Information Act Amendments*, Senate Report No. 93-1200, 93rd Congress, 2d Session, Washington, U.S. Govt. Print. Off., 1974, p. 12. The 1974 amendments (88 Stat. 1561) were passed over President Ford's veto, which was prompted partly by his view that provision for court review of agency classification decisions was unconstitutional. See *Weekly Compilation of Presidential Documents*, v. 10, October 21, 1974, p. 1318.

"The Court of Appeals in *Holy Spirit Association v. Central Intelligence Agency*, 636 F.2d 838 (D.C. Cir. 1980), affirmed a district court decision which ordered release of assertedly classified information, but that judgment was stayed by the Supreme Court and ultimately vacated as moot when the requesters withdrew their request for the classified documents. *Central Intelligence Agency v. Holy Spirit Association*, 102 S.Ct. 1626 (1982). The court in *Jaffe v. Central Intelligence Agency*, 516 F.Supp. 575 (D. D.C. 1981) quoted portions of classified documents in the course of its discussion of what it viewed as inconsistent classification decisions by the agency. Other district courts have ordered the release of classified information, but these orders did not survive either reconsideration or appellate review. See *Baez v. National Security Agency*, No. 76-1921 (D.D.C. Nov. 2, 1972), vacated on reconsideration, July 17, 1980; also see *Weberman v. National Security Agency*, 490 F.Supp. 9 (S.D.N.Y. 1980), reversed, 646 F.2d 563 (2d Cir. 1980), on remand, 507 F.Supp. 117 (S.D.N.Y. 1981), affirmed, 668 F.2d 676 (2d Cir. 1982).

"*Military Audit Project v. Casey*, 636 F.2d 724, 738 (D.C. Cir. 1981); *Lesar v. Department of Justice*, 636 F.2d 472 (D.C. Cir. 1980); *Hayden v. National Security Agency*, 608 F.2d 1381 (D.C. Cir. 1979), cert. denied, 446 U.S. 937 (1980).

"*Allen v. Central Intelligence Agency*, 636 F.2d 1287 (D.C. Cir. 1980).

"See *Sims v. Central Intelligence Agency*, 479 F.Supp. 84 (D.D.C. 1979), reversed on other grounds, 642 F.2d 562 (D.C. Cir. 1980); *Stein v. Federal Bureau of Investigation*, 662 F.2d 1247 (7th Cir. 1981); *Kanter v. Department of State*,

479 F.Supp. 921 (D.D.C. 1979).

"*Phillippi v. Central Intelligence Agency*, 546 F.2d 1009 (D.C. Cir. 1976); *Garrett v. Central Intelligence Agency*, 689 F.2d 1100 (D.C. Cir. 1982). E.O. 12356 requires (Section 3.4(f)(1)) an agency to refuse to confirm or deny the existence or non-existence of information requested under the F.O.I. Act whenever the fact of its existence or non-existence is itself classifiable under the order.

"*Baez v. Department of Justice*, 647 F.2d 1328 (D.C. Cir. 1980); *Lesar v. Department of Justice*, *supra* note 33.

"*Halperin v. Central Intelligence Agency*, 629 F.2d 144, 149 (D.C. Cir. 1980).

"See *Nawasky v. Central Intelligence Agency*, 499 F.Supp. 269 (S.D.N.Y. 1980); *Salisbury v. United States*, 690 F.2d 966 (U.C. Cir. 1982) (collecting cases).

"See *Kanter v. Department of State*, 479 F.Supp. 921, 923 n. 3 (D.D.C. 1979); *Marks v. Central Intelligence Agency*, No. 77-1108 (D.D.C. July 28, 1981); also see *Allen v. Central Intelligence Agency*, 516 F.Supp. 653 (D.D.C. 1981).

"*Baez v. Department of Justice*, *supra* note 37, p. 1336 n. 48.

"S.2452, introduced on April 28, 1982, by Sen. David Durenberger in reaction to E.O. 12356, would have amended the first exemption of the F.O.I. Act (5 U.S.C. 552(b)(1)) by applying it to matters that are "specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and are—(A) in fact properly classified pursuant to such Executive order, (B) matters the disclosure of which could reasonably be expected to cause identifiable damage to the national security, and (C) matters in which the need to protect the information outweighs the public interest in disclosure." Judicial review of subparagraph (C) would be limited to ascertaining whether or not the required balancing had been done by the agency. See *Congressional Record*, v. 128, April 28, 1982, pp. S4210-S4216.

This proposal would have reintroduced the balancing test and "identifiable" damage qualifier contained in E.O. 12065 into F.O.I. Act determination and litigation. Review of an agency's balancing decision, however, would be limited severely. Given this limitation and the seemingly relative insignificance of the modifier "identifiable," in terms of burden of proof in F.O.I. Act cases, the bill appears to be more of a signal to agency classifiers than an alteration of the standards of judicial review in F.O.I. Act cases involving exemption one. No action was taken on S.2452 during the 97th Congress.

"*Carlisle Tire & Rubber Company v. United States Customs Service*, 663 F.2d 210, 218 (D.C. Cir. 1980).

1983 CONVENTION, SEPTEMBER 21-24, 1983 HOTEL RESERVATION FORM, HYATT REGENCY LOUISVILLE

Mail To: Federal Bar Association, 1815 H Street N.W., Suite 408, Washington, DC 20006, Attention: Convention Secretary, no later than August 29, 1983 (thereafter rates and availability are subject to change)

Daily Rates (Check one and circle type of room)

Government Attorneys

\$46 Single or Double / twin

Non-Government Attorneys

\$41 Single or Double / twin

Reservation Guarantee: Reservations are held until 6 pm unless one night's deposit is received or guaranteed by credit card. Failure to cancel 24 hours prior to arrival will result in one night's charges billed to your credit card.

Hold until 6 pm only

Guaranteed by one of the following credit cards:

American Express

Carte Blanche

Discover

Continental

Diners Club

MasterCard

Deposit of \$ _____

Visa

Diners Club

MasterCard

Discover

Continental

American Express

Other _____

Expiration Date _____

Library Services Division

MICROFICHE RECORD
(Microfiched by the Master File Unit)

Initials

JALS

Date

3

18

83



SP
R
C

CONC
RESEARCH
SERV

AAAS BULLETIN

Scientific Freedom and National Security

Prepared by the Committee on Scientific Freedom and Responsibility

ISSUE 2

JUNE 1984

THE CURRENT DEBATE

At the 1984 Annual Meeting of the American Association for the Advancement of Science (AAAS), the Council of the AAAS passed the following resolution relating to scientific freedom and national security:

WHEREAS progress in science and technology is greatly enhanced by open communication; and

WHEREAS such progress promotes both the national security, however defined, and the general welfare; and

WHEREAS public availability of unclassified scientific and technical information is a necessity for democratic decision-making in a wide range of important public policy issues,

BE IT RESOLVED that the American Association for the Advancement of Science strongly reaffirms its opposition to continuing governmental efforts to restrict the communication or publication of unclassified research.

This statement of principle reaffirms a commitment made by the AAAS Council in a resolution passed during the AAAS Annual Meeting in January 1982. This earlier resolution stated that "Whereas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and the scientific process, . . . the AAAS opposes governmental restrictions on the dissemination, exchange, or availability of unclassified knowledge."

Both the 1982 resolution and the 1984 resolution were prompted by efforts that have been part of a drive by the Reagan Administration to prevent the export of U.S. technology to Soviet bloc countries. Restrictive efforts have included inhibiting communication of unclassified scientific research in university classrooms and research laboratories, in professional society meetings, and in scientific literature. Prepublication review and modification of unclassified technical papers, limitation of access by foreign students to university research projects and results, censorship of technical papers presented at professional society meetings, and restricting attendance at otherwise unclassified meetings to U.S. citizens have been among the means used by Administration officials to erect barriers against U.S. technology movement overseas.

The debate about restrictions on scientific communication has been closely monitored by the Committee on Scientific Freedom and Responsibility (CSFR) of the

AAAS. The Committee is chartered by the AAAS to monitor the policies and actions of the government of the United States, the governments of other nations, and private organizations, that circumscribe or restrict the freedom of scientists or restrict the ability of scientists to exercise their professional responsibilities as scientists. This is the second bulletin on scientific freedom and national security issues prepared by CSFR. The first bulletin was published in September 1982. The purpose of these bulletins is to keep interested persons informed about the evolution of new information control policies by reporting selected government and private activities which relate to this issue.

Much of the current activity within the Federal government relating to restrictions on scientific communication is concerned with two control mechanisms: export control laws and regulations, and research contract constraints. The principal regulatory instruments for controlling the flow of sensitive technical data across U.S. borders are the Export Administration Act, and the attendant Export Administration Regulations. The Export Administration Act came up for renewal during 1983, and has been extended under Executive Order 12470 pending Congressional revisions. Bills were passed in both Houses early in the second session of the 98th Congress. The Senate version contains more restrictive provisions than the House version. It is uncertain whether a conference version of the Export Administration Act of 1984 will be developed and passed before the end of the current session. One key issue is the wording of paragraph (12) of the revisions. The House version states national policy as follows:

It is the policy of the United States to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and other scholars to freely communicate their research findings by means of publication, teaching, conferences, and other forms of scholarly exchange.

The Senate version would substitute the words "involves sustaining" for "requires protecting," and insert the term "non-sensitive" before the words "research findings." There is a substantial difference in meaning between the two versions of the paragraph. Because "non-sensitive" is ambiguous, it could become the source of serious misuse, misunderstanding and controversy.

In the area of contract controls, a Steering Committee on Technology Transfer established within the Depart-

ment of Defense has made recommendations with regard to sensitive research undertaken in academic settings. "Non-sensitive" basic and exploratory research papers produced by DoD contractors can be submitted simultaneously to the contract officer and a publisher, with DoD having no right to require changes or to restrict publication. According to the recommendations, "sensitive" basic research papers should be submitted to the contract officer 60 days prior to submittal to a publisher, with the researcher retaining the option of whether or not to publish. "Sensitive" exploratory research papers should be submitted to the contract officer 90 days prior to submittal to a publisher, with DoD retaining the right either to require

changes before allowing publication or to block publication outright. A draft national policy on the transfer of scientific and technical information (see article below) makes the future of these recommendations unclear.

CSFR will continue to monitor these and other policy initiatives, and use these bulletins to report on the current debate. Future issues of this bulletin will provide a forum for presenting various perspectives in the national security/scientific communication debate. We welcome your comments.

Stephen Gould, Editor
Scientific Freedom and National Security

TO CLASSIFY OR NOT TO CLASSIFY—THAT MAY BE THE QUESTION FOR ACADEMIC RESEARCH

A directive establishing national policy for controlling the flow of scientific and technological information produced by colleges, universities and laboratories under contract to U.S. government agencies has appeared in draft form. Dr. Edith Martin, Deputy Under Secretary of Defense for Research and Engineering, made the draft available to the staff of the Committee on Science and Technology of the U.S. House of Representatives at a hearing on scientific communication and national security held 24 May 1984. According to the current version of the draft:

It is the policy of this administration that the mechanism for control of fundamental research in science and engineering at colleges, universities and laboratories under contract to U.S. government agencies is classification. Consistency of this policy with applicable U.S. statutes must be maintained. Each Federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant or contract and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants or contracts for potential classification. No restrictions may be placed upon the conduct or reporting of fundamental research that has not received national security classification.

The policy reportedly is the product of a 9 May 1984 meeting between Dr. George A. Keyworth, II, Director of the Office of Science and Technology Policy of the Executive Office of the President; William H. Taft, IV, Deputy Secretary of Defense; Fred C. Ikle, Under Secretary of Defense for Policy; Richard N. Perle, Assistant Secretary for International Security Policy; and Dr. Richard DeLauer, Under Secretary for Research and Engineering. The statement is being circulated among relevant Federal agencies, and may be subject to review by the National Security Council.

A background statement released as part of the draft notes that intelligence studies indicate a small but significant target of the Eastern Bloc intelligence gathering effort is science and engineering research performed at

universities and Federal laboratories. However, the policy recognizes that the "strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component."

Several important questions about the implications of the policy statement require clarification if the draft becomes final. One is the operational definition of the ambiguous term "fundamental research." Under Secretary DeLauer reportedly favors defining "fundamental research" to include all 6.1-research and 6.2-exploratory development work carried out at universities. Others in the DoD are said to be seeking a narrower definition.

The first sentence of the statement initially released to Congressional staff omitted the qualification "under contract to U.S. government agencies." Inclusion of this qualification in a subsequent draft leaves open the possibility that export control laws would still be applied to scientific and technological information produced by universities and laboratories with other types of sponsorship. The provision for "periodically reviewing all research grants or contracts for potential classification" could prove troublesome. This clause may allow classification of research results just prior to publication and dissemination.

Guidelines for classification that became effective in August 1982 reversed a trend towards making less information subject to the classification system. Executive Order 12356, issued by President Reagan, modifies a system established by predecessor orders dating back to November 1953. Information owned by the Federal Government, or under its control or produced by or for it, is to be considered for classification if it concerns scientific, technological, or economic matters relating to the national security, cryptography, or other matters that officials with original classification authority determine should be protected.

Although the main framework of E.O. 12356 is similar to the classification guidelines issued by President Carter (Executive Order 12065), the changes tend to make more information subject to the classification system. The threshold criterion for any classification under E.O. 12065

was whether disclosure could be expected to cause "identifiable damage" to national security. E.O. 12356 merely requires "damage." E.O. 12065 specified that if there was reasonable doubt as to the classification designation, or as to whether the information should be classified at all, the less restrictive designation should be used. E.O. 12356 deletes this provision, providing only that data as to which there is doubt shall be safeguarded at the higher level pending a determination within 30 days of the appropriate classification category. Unlike E.O. 12065, E.O. 12356 makes classification mandatory if disclosure of the information, either by itself or in the context of other information, meets the threshold for classification. While E.O. 12065 included certain time limits for classification, E.O. 12356 provides that information shall remain classified as long as required by national security.

After analyzing these and other provisions of E.O. 12356, the Committee on Government Operations of the U.S. House of Representatives concluded: "Given the past abuses of classification authority and the consistent pattern of overclassification by the executive branch, the Committee is not optimistic that classifiers will apply the new classification authority with restraint." Thus, while the draft policy on the transfer of scientific and technical information may be more clear-cut than alternatives such as application of export control laws, observers are not convinced that the policy represents a relaxation of efforts by the Reagan Administration to restrict communication of research fields that are currently unclassified.

BIBLIOGRAPHY

- Berkner, Lloyd V. "Secrecy and Scientific Progress," *Science*, v. 123, 4 May 1956, p. 783-786.
- Department of Defense. "A Report to the 98th Congress: The Technology Transfer Control Program." February 1984.
- Dertouzos, M.L. et al. *Interim Report of the Committee on The Changing Nature of Information*, Massachusetts Institute of Technology, February 1983.
- Ferguson, James R. "Scientific Freedom, National Security, and the First Amendment," *Science*, v. 221, 12 August 1983, pp. 620-624.
- National Academy of Sciences. *Scientific Communication and National Security*, (2 vol.) Washington, DC: National Academy Press, 1982.
- Nelkin, Dorothy. *Science as Intellectual Property: Who Controls Scientific Research?* New York: Macmillan, 1984.
- Relyea, Harold C. "Increased National Security Controls on Scientific Communication," *Government Information Quarterly*, vol. 1, no. 2, 1984, pp. 177-207.
- Rosenblum, R.A. et al. "Academic Freedom and the Classified Information System," *Science*, v. 219, 21 January 1983, pp. 257-259.
- Wallerstein, M.B. "Scientific Communication and National Security in 1984," *Science*, v. 224, 4 May 1984, pp. 460-466.
- Walsh, John. "DoD Springs Surprise on Secrecy Rules," *Science*, v. 224, 8 June 1984, p. 1081.

FYI

- According to James J. Harford, Executive Director of the American Institute of Aeronautics and Astronautics (AIAA), the absence of a clear-cut Department of Defense policy on restrictions of technical information is literally causing chaos among the professional engineering and scientific societies. Harford cites the experience of the AIAA, IEEE, the Society of Optical Instrumentation Engineers, the American Chemical Society, the American Vacuum Society, and the American Physical Society where sharp drop-offs in papers submitted for meetings and publications have occurred because authors are intimidated by DoD contracting monitors. Harford has initiated a new policy requiring AIAA Board approval of decisions to close AIAA meetings.

- A version of the Export Administration Act Amendments passed by the United States Senate (S.979) would require universities and colleges to report to the Secretary of Defense agreements with any agency of certain countries that result in the communication of unpublished technical data identified by the Secretary as involving a militarily critical technology. This could be interpreted to require that any transmission of unpublished data by faculty, through seminars, visits, colloquia and normal scientific discourse, that might involve certain technologies would first have to be approved by the Secretary of Defense.

- On 30 March 1984 the Department of Commerce published amendments to the Commodity Control List in the *Federal Register* as an interim rule with request for comments. "Certain types of technical data are added to a list of data requiring a validated license for export to all destinations except Canada. These data include, among others, technology specific to the production of 'superalloys,' and inert gas and vacuum atomizing technology." Section 379.4 is amended by revising the phrase—"No technical data relating to the following commodities"—in paragraph (d) to read—"No technical data relating to the following commodities or processes."

- The Governing Board of the National Academy of Sciences has approved formation of a new 20-member panel to do a follow-on study to the Corson Report. The proposed 18-month study will focus on the impact of national security controls on international technology transfer, particularly as they effect U.S. industry. Funding for the study is being sought from government agencies, professional societies, trade associations, and foundations.

- An editorial by William H. Gregory in *Aviation Week & Space Technology* (14 May 1984) reports that Europeans are considering a NOAMER policy for technical meetings held in Western Europe. According to Gregory, "Citizens of these countries have been personally affronted by the

THE VIEW FROM OSTP

The following is an excerpt from an interview of George A. Keyworth, II, Director of the Office of Science and Technology Policy, Executive Office of the President. The interview, conducted by Daniel S. Greenberg, was published in *Science & Government Report* (1 June 1984) and is re-printed with permission.

GREENBERG. The Defense Department . . . managed to create a lot of friction with universities on the issue of security and secrecy.

KEYWORTH. I don't think very many actions have been taken that have constrained the universities. Very little has actually happened.

GREENBERG. With (Richard) DeLauer (Under Secretary of Defense for Research and Engineering) on the way out, it would seem that the constraints are likely to increase.

KEYWORTH. I think that constraints on the university research environment through technology-transfer concerns of the government will be very, very few and will not in any way change the present academic environment.

GREENBERG. Do you think that the presidents of Stanford, MIT, and Caltech were overreacting when they wrote you and DeLauer about rules that might prohibit publication of some Defense-supported research?

KEYWORTH. They were overreacting in the sense that what they were afraid of was not a position that this Administration was likely to take. Their overall concern was a valid one. I sympathize with their concerns and I have all along. But the immediate fear they had at the time of the most stringent possible conceivable restraints being put on universities was unfounded and there weren't actions that had been taken. Their basic concern was justifiable. But I think the debate on tech transfer is a thing of the past. Why don't I just leave it there?

GREENBERG. It seems to be more active than ever. And you're saying it's been laid to rest? Stake through the heart?

KEYWORTH. I'm not sure that it has one heart, but I don't think there are going to be any constraints through technology transfer on the university environment that we don't have now.

GREENBERG. No more "US Citizens Only" signs at meetings that were previously open?

KEYWORTH. It's happened twice that I know of in three-and-a-half years. I won't say that it won't happen twice in the next three-and-a-half years. I don't think there has been any real impact on the academic environment to date, and I don't think there's going to be any in the future. Make a big deal out of it, if you want, but there have been two meetings, Photo-Optics and the Vacuum Society, where an arrest was made (of a visiting Eastern German researcher on espionage charges unrelated to the meeting) and when daylight came, no one criticized it. What there is is paranoia. No action has been taken that has been unsupportable, and what there has been is sheer paranoia over what might happen. Nothing has happened, and nothing is going to happen.

GREENBERG. Science attaches from friendly countries say their scientists are being denied admission to meetings here that used to be open.

KEYWORTH. We've probably had tens of thousands of meetings in this country in the last year, and I defy you to find five examples. I strongly suspect if you go back ten years, you'll find a comparable number. It's paranoia, it's ghosts.

GREENBERG. You're saying these are very rare events whose importance has been greatly exaggerated.

KEYWORTH. Exactly. I think that some of the debate that has occurred in government and that has fostered this paranoia will be resolved.

arrogance of the U.S. epitomized by the abbreviation NO-FORN"—restricting attendance at unclassified meetings in this country to U.S. citizens.

● David Packard, Chairman of the Board of Hewlett-Packard Company, made the following remarks in a speech before the IEEE Centennial Celebration on May 14, 1984: "I cannot resist the temptation to comment at this point on the grossly misguided current proposal by our Defense Department to censor the publication of the results of basic research funded by the Department at U.S. universities. They are also proposing to restrict technology transfer between the United States divisions and foreign divisions of international companies. I am quite certain that these proposals, if carried out, will do considerable damage to the advancement of all technology in the United States including technology useful for military purposes. It will not seriously hamper the Soviets in their progress in technology for military equipment unless an impregnable barrier can be placed around the Soviet Union and this, of

course, is impossible. To put the matter in plain English, the current effort of the Defense Department to censor basic research in the United States is simply stupid."

● Retired Admiral Bobby R. Inman, who warned the scientific community in 1982 of an impending crackdown on technical communication to halt "the hemorrhage of U.S. technology," is briefly quoted in a *Business Week* article (4 June 1984) as a voice of moderation. The article asserts that Richard N. Perle, Assistant Defense Secretary for international security policy, has become "the de facto czar of technology transfer in the U.S." in the absence of a national policy. According to Inman, Perle "is driving Defense, and he is taking a Fortress America approach that will not work." The article also quotes Dale R. Corson, president emeritus of Cornell University: "There are two things I'd like to see—a coherent (technology transfer) policy for the nation and a coherent policy that I believe in. I don't think we are likely to get either."

● At the AAAS Annual Meeting held in May, John

THE VIEW FROM DOD

The following is a discussion of the Department of Defense Steering Committee on National Security and Technology Transfer that appeared in "A Report to the 98th Congress: The Technology Transfer Control Program," dated February 1984.

This Committee has been working for almost a year on the effect of potential technology controls on U.S. science and industry. Chaired by the Deputy Under Secretary of Defense for Research and Advanced Technology, it is chartered to address four areas: academia, symposia, publications and emerging technologies. In these areas, it reviewed and recommended changes to current procedures, developed processes to simplify and systematize controls, and identified ways to increase the awareness of technology export problems to those concerned.

The Committee has developed a system for reviewing basic research papers which appears to be acceptable to both DoD and the university community. This system would not infringe on the right of university researchers to publish the results of their work. However, the Defense Department maintains the right to comment on proposed publications that result from DoD sponsored research. This ensures that the researcher is aware of any technology export concerns his publications may generate.

An instruction has been drafted on the sensitive issue of participation and attendance by DoD employees and contractors at unclassified scientific and technical meetings and conferences. The thrust of the guidance is that the Department of Defense will control participation by DoD employees and contractors according to the type of conference, but will not attempt to control the organization of the conference.

To simplify and aid the sharing of sensitive technical information within the Defense community, the Steering Committee devised a system for making technical documents. This system, now being implemented, shows the

extent to which documents may be distributed without additional approvals and authorizations.

Section 1217 of P.L. 98-94 gives the Secretary of Defense authority to withhold from public disclosure certain technical data. The purpose of the legislation is to protect sensitive, unclassified information previously vulnerable to public disclosure under the Freedom of Information Act and thus world-wide availability. The legislation applies to unclassified technical data with military or space application that is under DoD control and which may not be exported without U.S. Government approval. DoD Directive 5400.xx, drafted within the framework of the Steering Committee, will establish policy, procedures, and assign responsibilities for DoD implementation of this new authority. Disclosure of controlled technical data will be made to certified contractors or individuals who have agreed in writing to protect the information from public disclosure. The technical data will be available for bidding on future DoD contracts and foreign contracts for maintenance of U.S. originated systems. In implementing this authority, the Department will avoid stifling scientific research and will endeavor to assure that the authority is not used in a manner contrary to the intent of the Congress.

Other activities of the Steering Committee included developing alternative systems for monitoring emerging technologies for their military significance, exploring and promoting ways of increasing awareness of technology export control concerns, and developing methods for improving technical guidance in areas of technology that most deserve protection. In all of its activities, the Steering Committee has maintained open dialogs with industry, academia and professional societies to ensure that the concerns of all were heard. One of these activities, the DoD/University Forum, has proven so successful in this regard that it has been chartered as an official advisory body to DoD.

Birkner of the Defense Intelligence Agency predicted that "dual use" biotechnology (items with both peaceful and military applications) would sooner or later have to be brought under export control regulations. Charges that the Soviet Union is already exploiting biotechnology for biological warfare have emerged in recent weeks from official DoD sources, the Central Intelligence Agency, and a series of articles in the *Wall Street Journal*. Birkner asked scientists in industry and universities to help DoD learn "how our technology may be turned against us" so that a "prudent" list of militarily critical technologies can be compiled for biotechnology.

• The AAAS Committee on Scientific Freedom and Responsibility (CSFR) is sponsoring a Project on Secrecy and Openness in Scientific and Technical Communication which is well under way with three seminars already completed and six more projected for the fall. The project, under the guidance of Rosemary Chalk, CSFR Program Head, reviews a number of increased conflicts within the

scientific community over the dissemination of scientific and technical information. The seminars focus upon traditional concepts of scientific information as a public good, freely available to those who want access to it, as well as the many justifications used to limit access to new and important data, such as: economic conditions, national security interests and patent protections.

The project consists of a series of seminars and background papers. The papers are summarized at each session, followed by a prepared critique and general discussion. Topics thus far discussed have been: "Openness and Secrecy in Science: Their Origins and Limitations," "National Security Controls on Technological Knowledge: A Constitutional Perspective," and "Research as Intellectual Property: Influences within the University." Selected papers will be incorporated into a special issue of the quarterly journal *Science, Technology and Human Values*. For further information on the project, contact Sally Painter, CSFR, at the AAAS address.

EXCERPTS FROM THE MAY 24 HEARING ON SCIENTIFIC COMMUNICATIONS AND NATIONAL SECURITY

On 24 May 1984 the Subcommittee on Science, Research and Technology and the Subcommittee on Investigations and Oversight of the House Committee on Science and Technology held a joint hearing on scientific communications and national security issues. The following excerpts are taken from the written testimony submitted for the hearing record:

Dale R. Corson, President Emeritus, Cornell University

My (National Academy of Sciences) panel specified criteria for the identification of such "gray" areas . . . where we believed that research results should be neither classified nor totally available to everyone in the world. These criteria were the following:

1. The technology is developing rapidly, and the time from basic science to application is short;
2. The technology has identifiable direct military applications; or is dual-use (i.e. it has both civilian and military use) and involves process or production-related techniques;
3. Transfer of the technology would give the U.S.S.R. a significant near-term military advantage; and
4. The United States is the only source of information about the technology, or other friendly nations that could also be the source, have control systems as secure as ours.

We believed that the research fields meeting these criteria are few, in fact very few, in number. . . . Why not classify gray area research projects and guarantee security? The answer is three-fold:

1. To do so would seriously impede the progress of research in fields so classified; development activity can progress under classified conditions but basic research is inevitably slowed if the free exchange of information and ideas, which are so important to the nourishment of original thought, is impossible;
2. The major research universities are likely to abandon research fields where such classification is imposed, both because classification would impede progress and because classification is inconsistent with the academic environment; the case has not been made to the universities that there is a clear and present danger which demands classification of research on their campuses; and
3. Recognizing that more than half the nation's basic research is done in universities, and given the above circumstances, university research projects cannot be classified without serious damage.

(Editor's note: A Business Week article of 4 June 1984 reports that some Pentagon research officials who have been trying to convince universities to accept DoD sponsorship in critical research areas are unhappy with more restrictive policies. One veteran science administrator is quoted as stating "I think the problem will continue to get worse; there is no way you can attract universities back into defense research with this kind of boiling controversy.")

Paul E. Gray, President, Massachusetts Institute of Technology

Any efforts to control technology transfer will have some impact on the research enterprise. . . . The quality and integrity of research are anchored in its nature as a dispersed, interdependent, and cumulative enterprise. Research is dispersed in that work at the frontier, in most fields, is carried on simultaneously in several different locations. It is interdependent in that different investigators or groups of investigators rely on work done elsewhere to validate and extend their own work. The closer work is to the frontier of knowledge and the more swiftly a field is developing, the more researchers depend on open and rapid communication with colleagues working on similar problems elsewhere. This dependence leads to the development of informal networks of communication that rely on working papers, on preprints, and especially on personal communication. In a rapidly developing field, these informal mechanisms of communication assume the principal burden of communication among colleagues.

Research is cumulative in the sense that many small steps taken by individuals working in different places under different auspices contribute to new knowledge. Indeed, I would suggest that the leadership of the United States in fields as diverse as commercial cryptography and recombinant DNA has come about precisely because of the open, interdependent nature of research in American universities. In such endeavors, limitations on the communication of results obviously impede progress. I might also say that such secrecy is exceedingly difficult to achieve simply because so much of the communication that occurs is informal in character.

Thomas Ehrlich, Provost, University of Pennsylvania

Under the regulations implementing the Export Administration Act, universities are required to complete an extensive form concerning any Soviet scholar who seeks to come temporarily to the United States. One of the great strengths of the University of Pennsylvania is in biomedical electronics, and recently a Soviet scientist named Dr. Simakov applied to work in America on biomedical micro-sensors and processing systems. He listed University of Pennsylvania as his first choice. My colleagues in Penn's Center for Chemical Electronics think they could learn substantially from Dr. Simakov—at least as much, and probably more, than he could learn from us. Perhaps most important, working together in the realm of sensors, major developments may well occur. The area is recognized by the National Science Foundation as vital.

In order for Dr. Simakov to come, my colleagues would have to affirm that there would not be dissemination to him of information "directly and significantly related to design, production, and utilization in industrial processes." As a result, although Dr. Simakov could contribute greatly to work of enormous importance in this country, in all likelihood he will not be able to come. Ironically, I

understand we do not now have a clear picture of Soviet research efforts in the field of sensors. It would obviously be useful to have a window into that field at a major research institute within the Soviet Union. I am told that any potential transfer out of the United States would be small compared to the gain to the United States.

Roland W. Schmitt, Senior Vice President for Research and Development, General Electric Company

(Some of the changes now being proposed for technology export control would critically damage the American system that has heretofore led the world in the generation and application of new technology for both defense and civilian uses. Some of these proposals would halt the flow of technology to the Soviets by strongly impeding our own technical efforts, and ultimately crippling our own defense.

I'm referring specifically to the broad interpretation of the Export Administration Act of 1979 that has been proposed in informal draft regulations of the Department of Defense and Commerce. This interpretation would greatly restrict the amount of technical data that could be given to nationals of friendly countries—to students, employees, consultants, colleagues and customers of Americans. I remind you that it is release of technical data to citizens of friendly nations that is the key issue. Release of any unpublished data to nationals of the Eastern Bloc already requires government approval under existing regulations.

I'm also referring to attempts by the Department of Defense to exert new controls over access to unclassified research. For example, as a condition of supporting some unclassified research on millimeter wave transistors at Cornell University—research with defense implications, but that is a long way from practical application—the DoD specified that no foreign nationals work on the project; that nothing be published without DoD approval; and that no information be transferred to any foreign national. Although compromises were reached on the first two of these points, inability to agree on the third caused the procurement to be cancelled.

This new approach threatens to cause severe disruptions in our R and D capabilities. It would deny to our universities and our industries the capabilities of highly skilled foreign born scientists and engineers. It would isolate the U.S. from world science, alienate the science and engineering communities of our allies, and so provide the Soviets with both psychological and technological advantages. And it would enmesh our technological community in so much restriction and regulation that the productivity of defense research and development is sharply reduced.

Edith W. Martin, Deputy Under Secretary of Defense for Research and Engineering

To remedy the declining lead in military technologies, we can increase our efforts to advance technology, or we can attempt to slow down the flow of militarily useful technologies to our potential adversaries, or we can do both. It seems to me that doing both is necessary to increase our technology lead. Our goal in finding ways to

protect our technology has been to seek a balance which limits adversary access to our military technologies as much as possible while maintaining the ability of our nation to perform the research that gave us the technological lead in the first place. The litmus test of reasonableness in achieving that balance is the impact on U.S. technical superiority.

Until recently, the conduct of research in the universities had not caused significant concern with respect to the handling of Defense information. Most research, even that which has been funded by DoD, is unclassified. Most of the classified research performed by universities is conducted in "off-campus" institutions which, although affiliated with a university, are nonetheless separate enough so that strict security procedures can be employed.

More recently the situation has been complicated by other trends and changes: (1) The 1976 Bucy Report, "An Analysis of Export Control of U.S. Technology—A DoD Perspective," moved the focus of export controls from goods to the technology used to produce those goods. (2) It seems that some American universities are becoming more and more involved in applied and manufacturing technologies, e.g., microelectronics, and (3) it is becoming more and more difficult to distinguish between military and commercial technologies (e.g., computers, advanced materials, etc.)

The importance of universities as major performers in defense research and development is growing. About half of all defense basic research funds (budget category 6.1) are spent in universities, over \$400M in FY 1984. DoD relies upon and fosters university basic research and encourages dissemination of research results throughout the world scientific community in order to maximize the benefits of our investment. . . . Only a small portion of the unclassified work at universities is applied R&D that should be reviewed for military concerns. . . . We must fulfill DoD's mission by keeping our own technological capability well above that of our adversaries. We cannot afford to gratuitously build up an enemy's military or manufacturing technology base which might one day be used to damage or destroy our nation.

James S. Kane, Deputy Director of Energy Research, Department of Energy

DOE's current system of formal classification of technical information has worked well without imposing an onerous burden on the research enterprise. Section 148 of the Atomic Energy Act and the Nuclear Nonproliferation Act of 1978 have created carefully defined areas of unclassified, sensitive information that is controlled because of nuclear proliferation concerns, terrorists concerns, or obvious direct military applications. Attempts to create additional broad classes of "sensitive" information outside the formal system, particularly in the engineering or basic physical and biological sciences are inadvisable. DOE believes such attempts would more likely impede the progress that has given us technological superiority in the past, and it would place an enormous administrative burden on both researchers and their government sponsors.

The AAAS Bulletin on Scientific Freedom and National Security is published quarterly by the American Association for the Advancement of Science, 1515 Massachusetts Avenue, NW, Washington, D.C. 20005.

The Project on Scientific Communication and National Security is conducted on behalf of the AAAS Committee on Scientific Freedom and Responsibility. The Committee is authorized by the AAAS Board and Council to monitor the actions of the governments of the United States and other nations which circumscribe the freedom of scientists or restrict the ability of scientists to exercise their professional responsibilities, and to report on developments affecting scientific freedom and responsibility.

AAAS COMMITTEE ON SCIENTIFIC FREEDOM AND RESPONSIBILITY

Leonard M. Rieser, Chairman
Dartmouth College
Herman Pollack, Vice-Chair
George Washington University
Morris B. Abram
Paul Weiss, Rifkind, Wharton and
Garrison
Taft H. Broome, Jr.
Howard University
Mary M. Cheh
George Washington University
Thomas Eisner
Cornell University
Loren R. Graham
Massachusetts Institute of Technology

Arnost Kleinzeller
University of Pennsylvania
Robert E. Marshak
Virginia Polytechnic Institute
and State University
John M. Mulvey
Princeton University
Elena O. Nightingale
Carnegie Corporation of New York
Cristian Orrego
National Institutes of Health
Harold Relyea
Library of Congress
Alfred S. Sussman
University of Michigan

Chia-Wei Wuo
San Francisco State University
Anna J. Harrison (Board Representative)
Mount Holyoke College

AAAS Staff

Rosemary A. Chalk, Program Head
Eric Stover, Staff Officer
Stephen Gould, Editor and Project
Director
Kathie McCleskey, Program Associate
Sally Painter, Program Assistant
Linda Valentine, Administrative Secretary
Charles Hurteau, Secretary

CSFR Project on Scientific Communication and National Security
American Association for the Advancement of Science
1515 Massachusetts Avenue, NW
Washington DC 20005

NONPROFIT
ORGANIZATION
US POSTAGE
PAID
PERMIT NO. 7304
WASHINGTON DC

ACADEMIE

Federal Restrictions on Research *Academic Freedom and National Security*

The report which follows, prepared by a subcommittee of the Association's Committee A on Academic Freedom and Tenure, was approved for publication by Committee A at its meeting in June, 1982. It takes issue with attempted restrictions by the federal government on the open communication of nonclassified information for purposes of national security as a threat to academic freedom. Committee A, concerned that the federal government's Executive Order 12356 serves to encourage the classification of information as secret, has asked its subcommittee to prepare an additional report on the ramifications for academic freedom of classification by government agencies. Comments are welcome, and should be addressed to the Association's Washington Office.

Preservation of academic freedom has been a central concern of the American Association of University Professors throughout the organization's history. In recent years the federal government, in the cause of national security, has taken a series of actions which, in sum, represent a threat to academic

freedom. Even more worrisome is the trend toward increasing restrictions on research, foreshadowing not merely a threat to, but a significant infringement of, academic freedom. This report summarizes the experience of the last several years and questions the argument that the needs of national security require restrictions of academic freedom.

Actions of the Federal Government

Principally through classification and export control laws, but also by means of visa regulations, the federal government can restrain the flow of scientific and technological information which it considers would harm national security if made public.

Such restrictions have usually been applied to research carried out by governmental agencies and to the activities of private contractors who accept the government's secrecy requirements. However, during the past five years, national security concerns

have led the government to restrain the open communication of unclassified scientific information developed by researchers outside government. The Department of Commerce required that the American Vacuum Society withdraw invitations to East European scientists scheduled to attend an international conference on magnetic bubble memory devices. The Department of State notified organizers of a laser technology conference that eight Soviet scientists invited to a meeting in San Diego would be denied visas and that a Soviet postdoctoral researcher at the University of Texas, co-author of a paper submitted to the conference, could not travel to San Diego. The Department of State also asked the University of Minnesota to restrict access to unclassified information by a visiting scholar from the People's Republic of China in residence at the University. The University declined to cooperate. A request by the State Department through the National Academy of Sciences that a Soviet expert in robotics be similarly restrained when visiting Stanford University was also rebuffed. The State Department subsequently prevented the Soviet scientist from entering the country.

Statements by government officials have heightened concerns that government agencies are moving to restrict the free exchange of nonclassified scientific ideas. Admiral B. R. Inman, until recently Deputy Director of the Central Intelligence Agency, told a meeting of the American Association for the Advancement of Science that "publication of certain technical information could affect the national security in a harmful way," and cited information about crop projections and manufacturing processes as examples. The Deputy Secretary of Defense was more forceful: "Since the military posture of this nation relies so heavily on its technical leadership, the Defense Department views with alarm blatant and persistent attempts to siphon away our militarily related critical technologies." Even government voices which have sought to reassure the academic community have been edged with qualification. The Defense Department Science Board Task Force on University Responsiveness to National Security Requirements, in a report dated January, 1982, observed that the Department of Defense is "assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research." However, in its findings, the Science Board stated that "sensitive, nonclassified information should be subject to limitations on its distribution" taking into consideration the "special requirements for basic research."

Other initiatives, while not directly aimed at the academic community, underscore apprehensions that the government is seeking to impede the flow of nonclassified information. Notable among these developments is Executive Order 12356 (April 13, 1982), which expands the authority of government officials to classify information on broadened national security grounds. The executive order removes a previous requirement that decisions to classify information must be balanced against the public's right to know.

and provides that "if there is reasonable doubt about the need to classify . . . the information shall be considered classified."

In sum, the government, concerned that the open circulation of scientific ideas benefits our adversaries, principally the Soviet Union, to the disadvantage of the nation's security interests, has placed restrictions on foreign scientists and students invited to attend scientific meetings in this country, has tried to isolate visiting scholars and students at American universities from certain fields of research, and has suggested a broadened conception of threats to national security that appears to encompass research and teaching in our colleges and universities. The government has also adopted an executive order which makes it easier to classify information as secret.

Responses to These Actions

The academic community and others have reacted to these developments in a number of ways. In February, 1981, the Public Cryptography Study Group, convened by the American Council on Education with its membership drawn from the academic community and the National Security Agency, recommended a voluntary system of prior review of cryptology manuscripts, this in response to an assertion by the National Security Agency that some published information concerning cryptology could harm national security. The Mathematics and Computer Science Advisory Subcommittees of the National Science Foundation objected to the Study Group's recommendations as "unnecessary, unprecedented, and likely to cause damage to the ability and willingness of American research scientists to stay at the forefront of research in public sector uses of cryptography." The American Council on Education, the National Association of State Universities and Land-Grant Colleges, and the Association of American Universities have established with the Defense Department a University Forum to discuss mutual concerns, among them export control policies. The Forum is co-chaired by the president of Stanford University and the undersecretary of defense for research, and its other members are presidents of major research universities. The National Academy of Sciences has assembled a Panel on Scientific Communication and National Security, chaired by Dale Corson, to examine the relationship between university research and national security. The panel is expected to report by March, 1983. The Committee on Scientific Freedom and Responsibility of the American Association for the Advancement of Science, chaired by Leonard M. Rieser, is "exploring potential conflicts between national security interests and the traditions promoting the free exchange of unclassified research information within the scientific and engineering communities."

Academic Freedom and National Security

Academic freedom is the right to inquire, to teach, to speak, and to publish professionally. Some suggest that academic freedom is claimed as a special privilege

by self-interested professors, perhaps seeking, in Admiral Inman's words, to "immunize themselves from social responsibility." Academic freedom certainly benefits professors, but its primary purpose is to advance the general welfare. Learning, intellectual development, and progress—material, scientific, and technological—require freedom of thought, expression, and communication within colleges and universities, and the freedom to carry the results of inquiry beyond academic institutions. Academic freedom can scarcely fulfill its role in contributing to the general welfare, including national security, if those professionals engaged in research are prevented from learning the results of investigations carried out by colleagues in this country and abroad.

In our view, the public's interest in academic freedom may be compromised only when the open communication of nonclassified information poses great risks of substantial harm so immediate that there is no way to guard against them except by restricting such communication.

As we understand it, the government's position is as follows. The Soviet Union's military capabilities, quantitatively and qualitatively, have expanded at an alarming pace. We may have contributed to this expansion through the unfettered flow of scientific knowledge across national borders. Military power is highly dependent upon science and sophisticated technology, and high technology, whatever its source, can have military significance. Until recently, most research on technology related to the military was carried out by the government, by industry, and by a handful of research laboratories affiliated with universities but administratively, and often physically, separate from them (for example, the Livermore Laboratory at the University of California). The sources of scientific ideas potentially useful to our adversaries have grown with the military's reliance upon scientific information, additionally complicated by rapid strides in commercial technologies (for example, computers) which have national security applications. The present system for controlling the dissemination of militarily related information is suitable for dealing with the export of technical information aimed at preventing immediate military use of American technology by the Soviet Union. The pressing problem relates to unclassified scientific information developed by academic researchers: can ways be found to restrain the dissemination of only that research the disclosure of which could harm national security?

The government's position, as just described, warrants close attention. The margin of effectiveness provided to a nation's military power through technology may be crucial. However, the government does not claim, to the best of our knowledge, that the danger presented by the unhampered flow of unclassified information is the likelihood of sudden and disastrous gains by the Soviet Union. Rather it contends that scientific information may help the Soviet Union improve industries which in turn provide support for the development of weapons. On the basis of these conjectures the case for restraining academic freedom is not convincing. Were we to

accept the long-term considerations which the government seems to advance as appropriate reasons for limiting the exercise of academic freedom, claims on behalf of national security no matter how broad or indefinite could be used to justify any manner of restraints on academic freedom at any time. The likely result would be permanent damage to society's interest in academic freedom.

Moreover, if we keep in mind the large volume of scientific information and advanced technology obtained by the Soviet Union from West Germany, France, Sweden, Japan, and other countries, it is unclear how restraining the flow of unclassified information can achieve its objective of retarding, let alone preventing, Soviet military advances. Such restraints would more likely hinder our own progress in military-related technology than they would hamper the progress of potential enemies. We note also that by the government's own estimates, Soviet technology has profited far more from the importation (both legal and illegal) of hardware from the West than from ideas appearing in the open literature.

An academic researcher who makes a discovery which it is believed could harm the nation's security if obtained by an adversary undoubtedly has a moral obligation to society to inform the government of what has been discovered prior to publication. The record of college and university researchers as a group does not justify the suspicion that they will not act responsibly in this regard. Attempts to codify such moral obligations, whether through legislation, administrative regulation, or other means, are not likely to succeed in their primary purpose and are likely to do considerable damage, both to our traditions of openness and to the effectiveness of our scientific and engineering efforts.

We are mindful of the risks that may accompany the exercise of academic freedom. But there is the major hazard of discouraging imagination, thought, and inquiry. It is from vigorous intellectual combat that new ideas emerge. The trial and error of searching for truth, of challenging settled habits of thinking and proposing fresh hypotheses which themselves may call forth ideas that displace them, is the crucially distinctive quality of the university as a community of scholars. Restraints or pressures by outside authorities inhibit the free and spirited exchanges which underlie advances in scholarship and discoveries through research. The path to safety lies in the opportunity to discuss ideas freely. The need is for more academic freedom, not less.

ROBERT A. ROSENBAUM (Mathematics),
Wesleyan University, Chair

MORTON J. TENZER (Political Science),
University of Connecticut

STEPHEN H. UNGER (Computer Science),
Columbia University

WILLIAM VAN ALSTYNE (Law),
Duke University

JONATHAN KNIGHT, Staff

SPECIAL REPORT

Information control I

Technology transfer at issue: the academic viewpoint

Educators believe efforts to limit transfer of knowledge at the university level are likely to weaken the U.S. lead in innovation

Confronted by increasing commercial competition from Western Europe and Japan in high-technology markets, as well as by heightened tensions in relations with the Soviet Union, the United States has taken a new and vigorous interest in controlling the flow of technology outside its borders. There is growing concern in the Federal government that the "leaking" of technical material and ideas to other nations impairs national security both by diminishing the ability of the U.S. to compete commercially and by reducing the country's edge in armaments. Yet specific efforts that have been initiated to control technology transfer in the university setting are themselves likely to weaken the U.S. position and thus do not serve national interest.

Among these efforts have been controls on cryptography, voluntary up until now, and on technical information and scientific exchanges. Such curbs have been imposed through the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), and the Department of Defense has proposed restrictions on research carried out under the Very High Speed Integrated Circuits (VHSIC) program.

Some say that universities simply must learn to live with new constraints if they wish to do research in "sensitive" areas. The likely response from many faculties would be a decision not to undertake such research. If this occurs, both the university and the nation will suffer, and there will soon be fewer ideas and developments worth protecting. If the list of sensitive areas is as broadly drawn as Admiral Bobby Inman, deputy director of the Central Intelligence Agency, has suggested, the U.S. will be severely damaged.

An alternative approach would be to draw a much narrower list of areas to be protected and to classify all research in those areas, regardless of where it is performed. This would have the advantage of presenting universities with a clear choice. Some appraisal of the potential cost—in terms of wasted effort and lost effectiveness—could be made, and these costs could be compared with those associated with leakage of the research. But there should be much public discussion before any restrictive regulations are recommended.

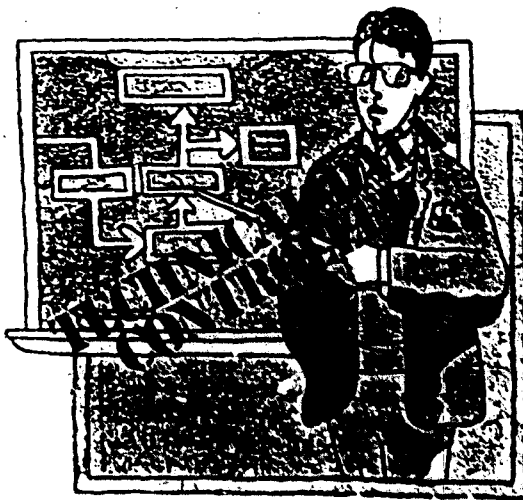
Restrictions came with World War II

The idea that university research should be restricted by the Government did not take hold seriously until World War II. For more than a century research has been a feature of U.S. university life. Before the second World War, there was little Federal involvement; the small amount of sponsored research in the universities was supported largely by industry and was usually narrow in scope and applications-oriented. But the war involved

many scientists and engineers in the application of technology to military purposes.

These researchers, drawn mostly from university faculties and often placed in university laboratories organized for specific military purposes, were deeply engaged in developing microwave radar, high-frequency communications systems, automatic fire-control systems, navigational aids, and jet-aircraft design, to say nothing of nuclear weapons. Their projects were, of course, classified. Secrecy was accepted for the short term as essential to winning the war, and it produced little conflict within the universities at that time—because of the urgency of the war effort and, most significantly, because the paucity of students during those years resulted in a virtual suspension of their educational efforts. Universities, in short, stopped functioning as universities.

During the years immediately following the war, the Government and the universities developed arrangements that made possible continued Federal support of basic research in university settings. Most of those developments had their roots in a report prepared in 1945 by Vannevar Bush, who during the war was science advisor to Presidents Franklin D. Roosevelt and Harry S. Truman. Dr. Bush's report, *Science, the Endless Frontier*, recommended the creation of the National Science Foundation, which Congress established in 1950. During those immediate postwar years other Federal agencies, including particularly elements of the DOD, established their own patterns of support for



(Teach to U.S. citizens only.)

Paul E. Gray
Massachusetts Institute of Technology

basic research in universities. Several considerations led to this postwar partnership:

- The wartime experience had shown that universities had much to contribute to basic and applied research and that university faculties were an enormously valuable national resource.
- Basic research was becoming far more complex and costly. Industry viewed it as a high-risk venture, since its benefits were returned primarily to the common account. It was clear that the Federal government would have to become its principal patron.
- The Government had an interest—and the nation a high stake—in the education, through the postdoctorate level, of more scientists and engineers, and the academic environment of the research universities was uniquely equipped to develop these human resources.

Research thrives in openness

As this new partnership developed, the curtain of secrecy that had surrounded Government-sponsored university research during the war was lifted. Research in universities was usually performed without limitations on access or the dissemination of results. This shift to openness, which had long characterized university-based research, was undertaken quite deliberately, and the reasons for it are fundamental to any understanding of the consequences of present restrictive efforts.

The quality and integrity of research are anchored in its nature as a dispersed, interdependent, and cumulative enterprise. Research is *dispersed*, in that work at the frontier in most fields is carried on simultaneously in several locations. It is *interdependent* in that different investigators or groups of investigators rely on work done elsewhere to validate and extend their own work. The closer work is to the frontier of knowledge and the more swiftly a field is developing, the more researchers depend on open and rapid communication with colleagues working on similar problems elsewhere. This dependence leads to the development of informal networks of communication that rely on working papers, preprints, and especially personal communications. In a rapidly developing field, these informal mechanisms assume the principal burden of active communication among colleagues. The refereed journals of science become the publications of record, but they are not the primary means for communicating innovation.

Research is *cumulative* in the sense that many small steps, taken by individuals working in many different places and under diverse auspices, contribute to new knowledge. Indeed, the leadership of the U.S. in such diverse fields as cryptography and recombinant DNA, for example, has come about precisely because of the open, interdependent nature of research in American universities. In such endeavors limitations on the communication of results obviously impede progress. Such secrecy is also exceedingly difficult to achieve.

The crucial dependence of research on openness and communication among co-workers was recently expressed most cogently by Sissela Bok, lecturer on medical ethics at the Harvard Medical School and the Harvard-Massachusetts Institute of Technology Division of Health Sciences and Technology:

"The felt need to take a stand against secrecy also springs from concern for what is most central to the scientific enterprise itself: from a recognition of the damage that secrecy can do to thinking, to creativity, and thus to every form of scientific inquiry. Because secrecy limits feedback and restricts the flow of knowledge, it hampers the scientists' capacity to correct estimates according to new information, to see connections, to take unexpected leaps of thought. And secrecy is expensive in that it fosters needless duplication of efforts, postpones the discovery of errors, and

leaves the mediocre without criticism and peer review. Secrecy therefore can cut into the quality of research and slow scientific momentum." (See *Science, Technology, and Human Values*, Vol. 7, no. 38, Winter 1982, p. 33.)

Scientific research is, increasingly, an international undertaking. Talent and creative energy are widely distributed and do not respect political and national boundaries. Thus world-class research in many fields is done in Western Europe, in Japan, and in the Soviet Union, as well as in North America and many other places. Furthermore the faculties and research staffs in most U.S. universities are composed in part of scholars from many other countries. Some are here more or less permanently; others are visitors for a few weeks or a few years. Academic and other institutions achieve prominence in research by focusing in a single-minded, insistent, passionate way on attracting and retaining the most creative individuals. This inevitably leads to a cosmopolitan community at all of our great research universities.

These universities are unique in their intimate coupling of education and research. Thus faculty members engage regularly in conventional teaching and also in research, which itself embodies many of the essential elements of teaching in a less formal setting. Both undergraduate and graduate students do research, contributing the enthusiasm and intellectual energy of youth and the special advantage of not knowing that "it cannot be done that way." Curricula are revised and kept current by the steady infusion of ideas developed in the research laboratories.

The complete enterprise is much more than the sum of the parts—education and research—and the resulting synergism is a major factor in the outstanding achievements of academic science in the United States. Any effort to decouple education and research will diminish both activities and weaken our national position.

Restricting classified research

These characteristics of scientific and technical research influenced the postwar decision to reestablish research in universities in open settings. Universities and the Federal government developed an understanding that basic scientific research not directly related to the national security would be undertaken in an unrestricted environment. As part of this understanding, universities have undertaken classified research only after careful and detailed consultations with the Government on both the need for the research and its scope. When such research is undertaken, it is usually carried out at sites separated from the university campus and isolated from the normal academic environment and process.

Further, after the fact classification of research results has been rare. This pattern was developed not to indulge our academics, but out of a shared understanding of the quality and the effectiveness of research conducted in an open environment.

An underlying premise of this shared understanding was that, except for classified research, the traditional academic freedoms of inquiry, teaching, and publication would not be abridged. A university or its research faculty may agree by contract, of course, to a system of prior review, but unless such an agreement is in force, there remains a constitutionally protected right of publication. And the progress of science, as noted, has clearly been advanced by this understanding and this basic First Amendment protection.

Concern in academia spreads

My own growing concern about the application of controls to research in academic settings has its roots in a controversy regarding the national security implications of research in cryp-

tography—research connected to several interesting problems in abstract mathematics. Many scholars working in the general area of computer science see the need for secure, convenient cryptographic systems to protect the growing volume of personal, business, and other information stored in and processed by computers, often operating in large-scale networks. However, the civilian and domestic interest in developing secure and convenient cryptographic systems may come into conflict with the interests of Federal agencies in protecting the security of U.S. Government communications and in extracting useful intelligence from other communications.

This tension led the American Council on Education, with the encouragement of the National Security Agency, to form the Public Cryptography Study Group. This committee recommended, late in 1980, that researchers voluntarily submit papers on cryptography to the agency for review prior to publication. It is not clear what actions will be taken by the NSA, or requested of the researcher, if a submitted paper is deemed to contain sensitive material. It appears that some persons doing research in cryptography are following this recommendation; others, including several at MIT, have *not* agreed to a process of automatic prior review, even though, since 1977, they have been sending the NSA prepublication copies of all cryptographic papers at the time they are sent to close colleagues for technical comment [for information gathered on the program by *Spectrum*, see "Cryptography: voluntary control seems to work," below].

Now the concerns have spread beyond cryptography to em-

brace regulations related to export control. These latter regulations deal with unclassified material and have been in place for some time; however, efforts to apply them to work done in universities have become apparent only recently. Thus the present state of affairs is in flux and somewhat confused.

In December 1980 the director of the DOD's VHSIC program informed scientists working for the program in universities that devices and technical data developed by contractors under the program would be subject to the International Traffic in Arms Regulations, administered by the State Department in consultation with the DOD, and the Export Administration Regulations, administered by the Department of Commerce. The memorandum from the VHSIC director that attempted to define the category of controlled technical data stated in part:

"Controlled technical data does not include information normally considered to be basic science, such as information related to materials properties, physical and chemical reactions, fundamental physical limitations, stress analysis, statistical inference, device physics, and other such products of basic research.... The distinction that is being made is between basic research and process, or utilization, technology. The former are not subject to controls, while the latter are."

The memorandum went on to say:

"In the case of basic research supported by the VHSIC program, *although such research and its results are not generally controlled* [emphasis added], it is the preference of the Program Office that only U.S. citizens and immigrant aliens who have

Cryptography: voluntary control seems to work

No one is certain just how mandatory controls on research and publications would affect academia or industry, but the experience of researchers in cryptography may offer some guidelines on voluntary controls.

As university studies in cryptography and related areas of mathematics grew in the U.S. during the 1970s, the National Security Agency (NSA), which is responsible for code making and code breaking in the Government, became concerned that private research might impinge on its domain, with grave implications for intelligence gathering. In 1975 the NSA suggested to the National Science Foundation that the NSA have sole responsibility for funding cryptological research. The foundation rejected this suggestion, but it did agree to include NSA representatives among the reviewers of grant proposals in cryptography.

In 1977 an NSA employee, apparently acting on his own, wrote a letter to the IEEE warning that papers to be presented at an upcoming symposium might violate the International Traffic in Arms Regulations by disclosing information on the U.S. munitions list. That list includes "speech scramblers, privacy devices, cryptographic devices (encoding and decoding)," and any information relating to their design, construction, and operation. The symposium was held without incident, although some papers written by graduate students were presented by their professors to shield them from legal repercussions.

Also in 1977, two patent applications for encryption and scrambling devices were seized by the Government under the Patent Secrecy Act of 1952; this action was taken at the request of the NSA. After protests from cryptographic specialists, the two secrecy orders were withdrawn in 1978.

In 1980, Leonard Adleman, a researcher at MIT, was informed that a portion of his National Science Foundation grant would not be renewed because it impinged on national security concerns. Shortly thereafter the National Security Agency offered to support the work, but Dr. Adleman refused. Eventually the original grant was restored in full.

In the meantime the Public Cryptography Study Group, a

collection of experts from the NSA and academia, had been set up to look at the problem of unclassified research in cryptography and its implications for both national security and academic freedom. The group recommended the establishment, on a trial basis, of a voluntary review program in which authors would submit papers to the security agency for an opinion before publishing them, although the final decision on what to publish would rest with the authors. This program is now operating, although not all researchers use it.

One conclusion that the cryptography study group came to was that a legislative, mandatory program was not needed—and would, in fact, be counterproductive. Martin Hellman, a cryptographer at Stanford University, points out that it would be almost impossible to get more than superficial compliance with a mandatory system. Dr. Hellman adds that voluntary controls should work well "because at present there are no real controls on us, and so the NSA will have to behave reasonably to gain support for its program."

One case of the voluntary system in action was recently reported to *Spectrum* by a noted cryptographer, who asked that his name not be used. He said that a colleague had come to an agreement with the NSA to delay publication of a paper. Even though it went against the grain of academic thinking to delay publication, the researcher was glad that the NSA had brought the national security implications of the paper to his attention.

According to this source, the security agency did not coerce the researcher, but rather insisted that he was free to publish if he so desired. The NSA simply explained to him the reasons why it felt the paper should not be published immediately. Although the length of the delay was not reported, the source indicated from his own discussions with the NSA that such delays are intended to allow other researchers to catch up with major advances, so their principles can be rediscovered independently.

In the case at issue, the NSA apparently expects other researchers to come up with the same idea within a few years.

—Paul Wehr

declared their intention of becoming citizens participate. Where this preference cannot be accommodated, the contractor should be directed to the Program Office for resolution."

The memorandum made a set of distinctions between basic and applied research that were, at best, not particularly helpful in a field where the most fundamental and important research at present may be that relating to design methodology and the use of artificial intelligence in the creation of new design tools—work that might fail the test as "basic science."

It also proposed restrictions—applicable even to basic research—that disregard both the international character of U.S. universities and the difficulties such institutions would have in confining participation in and access to research to U.S. citizens and immigrant aliens.

Five university presidents give warning

Early in 1981 the presidents of five universities heavily involved in such work—the California Institute of Technology, Stanford University, Cornell University, the University of California system, and the Massachusetts Institute of Technology—wrote to the secretaries of commerce, defense, and state to express concern and request clarification concerning this and similar attempts to apply the arms and export regulations to university-based research. The letter said in part:

"The new construction of these regulations appears to contemplate Government restrictions of research publications and of discourse among scholars, as well as discrimination based on nationality in the employment of faculty and the admission of students and visiting scholars. In the broad scientific and technical areas defined in the regulations, faculty could not conduct classroom lectures when foreign visitors were present, engage in the exchange of information with foreign visitors, present papers or participate in discussions at symposia and conferences where foreign nationals were present, employ foreign nationals to work in their laboratories or publish research findings in the open literature. Nor could universities, in effect, admit foreign nationals to graduate studies in these areas. Such restrictions would conflict with the fundamental precepts that define the role and nature of this nation's universities....

"Restricting the free flow of information among scientists and engineers would alter fundamentally the system that produced the scientific and technological lead that the Government is now trying to protect, and leave us with nothing to protect in the very near future. The way to protect that lead is to make sure that the country's best talent is encouraged to work in the relevant areas, not to try to build a wall around past discoveries."

For nearly a year now there has been a review of these issues and concerns under the auspices of the Department of Defense. The conclusions of that review are not yet apparent.

Earlier this year in Washington during the annual meeting of the American Association for the Advancement of Science, a panel discussion on this general subject was held, entitled "Striking a Balance: Scientific Freedom and National Security." Admiral Inman, the CIA's deputy director, was a participant. In his paper, "National Security and Technical Information," he referred to the tension that results from the "overlap between technical information and national security" and he urged that researchers join with Government to find a suitable balance that would "simultaneously protect the nation and protect the individual rights of scientists—both as academicians and citizens." Admiral Inman concluded that restrictions imposed in the interest of national security are necessary.

"Scientists do not immunize themselves from social responsibility simply because they are engaged in a scientific pursuit,"



(May not participate in or learn about advanced applied research.)

he said. "Society has recognized over time that certain kinds of scientific inquiry can endanger society as a whole and has applied either directly, or through scientific/ethical constraints, restriction on the kind and amount of research that can be done in those areas."

Admiral Inman suggested that the system of voluntary prior review developed by the Public Cryptography Study Group might be workable. In the discussion that followed the prepared statements, the admiral was reported in the press to have predicted a "tidal wave" of public outrage and laws "restricting scientists if scientists do not agree voluntarily to review of their work by intelligence agencies." He proposed requiring such review in the fields of "computer hardware and software, other electronic gear and techniques, lasers, crop production and manufacturing procedures."

Reagan proposes tighter restriction

In the weeks following Admiral Inman's remarks, similar concerns about the consequences of "leaks" of technology were expressed by the secretary of defense, Caspar Weinberger, and the deputy secretary of defense, Frank Carlucci. Recently President Reagan issued an order superseding the former Executive Order 12065 concerning security classification. The changes are many, but the following are most significant for universities:

- Information shall be "safeguarded as if it were classified" if there is a "reasonable doubt" about the need to classify. Though this standard may be workable for Government officials, it most surely is not for university researchers. The "reasonable doubt" standard puts those engaged in university research in a perilous quandary, and the new rule represents a reversal of earlier policy in doubtful situations.

- The prior exception for the results of non-Government research and development is eliminated. This suggests that the revised Executive Order purports to reach the results of non-Government research if the classifying authority determines that the product incorporates classified information—whether or not the researcher had access to any classified information.

Earlier drafts of the Executive Order also threatened to eliminate the prior exception for "basic scientific research not clearly related to the national security."

It may be, of course, that the conjunction of these statements and actions, both real and threatened, reflects more coincidence than coordination. However, it is not difficult to understand why many involved in research and education in universities are deeply concerned that in the name of national security the stage has been set for the imposition of controls on the flow of information within universities—controls that would seriously affect the climate and operation of these institutions and the great benefits issuing from them to the nation.

A balanced assessment is needed

The unintended transfer of technology to other nations is said to be a serious problem for U.S. national security. University scientists can form no independent judgment of the magnitude of this threat, of course, because the data essential to an informed judgment are, perforce, classified. Further, it is said that universities contribute to this unintended transfer of technology through their international communities of students, faculty, and research staff; through the publication of results in the open literature; and through the intrinsic openness of university communities.

Even if this were so, which is far from clear, any potential disadvantage must be measured against the very great advantage to scientific progress, and to the nation, of open and unrestricted research. There is also a question of how significant the "leaks" from universities are compared with those connected with the licensed export of dual-use technologies, from the theft or unlicensed sale of restricted technologies, from the operations of multinational companies, from disclosure to friendly nations, and so on.

We urgently need a balanced and reasoned assessment of this issue in light of that question, so that legitimate efforts to restrict the transfer of technology from the universities will be based on proper analysis of the problem, a full understanding of how progress in science evolves, and an appreciation of the possible unintended consequences of constraints.

For example, prepublication reviews of sensitive information will not, by themselves, work very well because of the informal communication networks among researchers. Effective control of the dissemination of results would have to be exercised at a much earlier stage in the research process. It would mean that researchers and visitors would have to pass some sort of reliability

test or be excluded from a project. And it would mean the abandonment of the informal communications network that is central to progress and quality in research.

Such conditions may be met in the setting of a Government laboratory or a corporate research facility, but they are entirely foreign to universities, where research and education are inextricably entwined, where talent and creativity are sought and developed without regard to national origin, where few doors are locked, and where activities are not sequestered.

The suggestion that universities already have working arrangements with corporations that apply this kind of constraint to privately sponsored research is simply wrong. Though many universities are prepared to accept support from both corporations and Government when such support involves brief delays of publication to permit protection of intellectual property rights, few universities, I believe, would be prepared to undertake research that is proprietary to a sponsor and that cannot be freely described and reported.

It is to be hoped that the costs and benefits of all possible constraints will be most carefully weighed in the national debate now arising over this complex issue. Further, the larger progress of U.S. science and technology and their indissoluble international aspects should be weighed carefully in this debate against short-term policy objectives in this debate.

It is encouraging in this regard that there has recently been established a new joint committee by the Department of Defense and the Association of American Universities to conduct such a review. A similar study is also being undertaken by the National Academy of Sciences. It is quite possible that these and other studies could, within a reasonable amount of time, formulate specific recommendations to serve both the cause of national security and the larger progress of science and technology in the broad national interest.

To probe further

For further information on academic responses to perceived national security needs for secrecy, see "Secrecy and Openness in Science: Ethical Considerations," by Sissela Bok (*Science, Technology and Human Values*, Vol. 7, no. 38, Winter 1982). An overview of institutional concerns may be found in the report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements, released March 5, 1982, by the Office of the Under Secretary of Defense for Research and Engineering, Washington, D.C. 20301. The report also examines what increases in support may be necessary to fulfill the nation's need for scientists and engineers.

Also of interest regarding information controls is a speech by Representative George E. Brown (D-Calif.) in the Congressional Record for Feb. 25, 1982, p. H 511.

About the author

Paul E. Gray is president of the Massachusetts Institute of Technology, Cambridge. Prior to assuming the presidency, Dr. Gray was chancellor of MIT from 1971 to 1980, and prior to that, professor of electrical engineering. Dr. Gray's primary interest as a researcher was in semiconductor devices and circuit theory. He has also taken an active role in shaping engineering education, as teacher as well as chancellor and president; in 1968, he was appointed to a chair at MIT established "for the purpose of rewarding and encouraging superlative teaching."

Except for two years in the Army Signal Corps, Dr. Gray has spent his entire professional life at MIT. He received a B.S. in 1954, an M.S. in 1955, and a D.Sc. in 1960 and began teaching at MIT in 1957. ◆



(Requires license for publication.)

SPECIAL REPORT

Information control II

Technology transfer at issue: the industry viewpoint

Economics makes industry a cautious ally in academia's fight against U.S. government attempts to stem the free flow of ideas

The deputy director of the Central Intelligence Agency told scientists and engineers at a meeting of the American Association for the Advancement of Science on Jan. 7, 1982, that they must control the exportation of technical information voluntarily or face legislative action that will "slam shut" the door through which United States expertise is reaching military and economic adversaries. "In terms of harm to the national interest," the CIA official said, "it makes little difference whether the data is copied from technical journals in a library or given away... to an agent of a foreign power."

A month later Senator Henry Jackson (D-Wash.) called on the Senate floor for increased controls on technical information and scientific exchanges.

As the U.S. continues to slip in the world marketplace and U.S. companies find themselves losing to foreign competitors even at home, controls or threats of controls on information have increased. While most companies would not argue with the general goal of curbing information on exclusive industrial processes and designs—most have no intention of releasing that in the first place—some industry executives take exception to the way the Government is enforcing its controls.

When the Control Data Corp. of Minneapolis, Minn., tried to sell a Cyber 172 computer to the Soviet Union, for example, it followed the rules to the letter and ended up in frustration. Most companies that export products or information report some trouble with export regulations. Even Texas Instruments Inc., Dallas, whose president, J. Fred Bucy, has been influential in attempts to tighten controls on technical information, admits the regulations impose an administrative burden. "But we don't find that a major constraint," James Dukowitz, manager of government relations at TI, hastened to add. "We believe in controlling the flow of technology to adversary nations."

In the case of Control Data, the constraint has tried the company's patience. Control Data got an export license for its Cyber 172 in December 1979. The computer was flown to Frankfurt, West Germany, and from there it was to be trucked to Moscow. But by the time it was loaded onto a truck, the United States had declared an embargo on trade with the Soviet Union because of the latter's invasion of Afghanistan.

"We asked the Department of Commerce what to do about our export license," related Robert Schmidt, vice chairman of Control Data. "They told us to send it back. So we left the computer in Frankfurt. All through 1980 and 1981 it sat in a warehouse."

When the Reagan administration took office, Control Data reapplied for permission to export the machine, but got no answer. "We asked them again in November '81, and we still

haven't heard anything," Mr. Schmidt said. "The machine is still in the warehouse, but we've told the Soviets we won't be able to get permission to ship it. We've decided to sell it to the West."

Mr. Schmidt is particularly concerned because the company's queries have gone unanswered. "There doesn't seem to be anybody at DOD or State who understands what this is doing to industry and the U.S. economy," he said.

A new Executive Order does little to alleviate the fears of Mr. Schmidt and others in industry who are wary of controls. The order removes restrictions on classification of privately funded applied research and states that, if there is doubt whether material should be classified, it must be treated as classified until doubts are resolved.

The order would also eliminate balancing of public need to know against the Government's desire for secrecy, and it would end all limits on the length of time that material could remain secret without a review for declassification. Are such sweeping powers necessary? To get some insight into the Government's view, one must go back to the "Bucy Report" of 1976.

The case for controls

Government fears over the export of technical information were made public in the "Bucy Report," a study by the Defense Science Board. The panel doing the study, headed by TI's president Bucy, concluded that the U.S. was losing its technological and economic lead over adversaries by giving them the expertise critical to the production of advanced devices. The report recommended stricter control of the flow of information.

In late 1979, Eugene E. Yore, U.S. Army deputy for science and technology to the assistant secretary for research, development, and acquisition, said: "At present we are technologically inferior to the USSR in almost every major fielded system."

"Much of the leakage of the last decade came because détente brought liberalization of controls on trade with the Communist countries," says Vincent F. DeCain, acting director of the Office of Export Administration in the Commerce Department. "The result of that liberalization is that we must now shoulder an enormous defense budget to regain our position."

In addition to spending for innovation and additional hardware, Mr. DeCain said, the United States must also assume control of its technological base. This will require a closer look at the export of not only design and manufacturing processes, but also "keystone equipment"—devices that perform some critical step in manufacture and thus have technical information built into them. "Any product or any technology that provides the Soviets with greater ability in production or design will be given greater scrutiny," he says.

Control of technical information in the U.S. is currently exercised through two major bodies of regulations: the Export Administration Regulations (EAR), administered by the Commerce

Paul Wallich Associate Editor

Department, and the International Traffic in Arms Regulations (ITAR), administered by the State Department.

The Departments of State, Commerce, and Defense consult each other on sensitive license applications under either set of regulations, but while the Commerce Department has expediting procedures for licensing, the State Department does not. And the State Department is considered more likely simply to follow the recommendations of the Department of Defense on licensing decisions. The DOD uses its Military Critical Technologies List, a classified document, as a reference for making recommendations to either the Commerce or State Departments.

Other Western nations have controls on technology transfer but tend to enforce them differently. The Coordinating Committee on Export Controls (CoCom), which consists of countries in the North Atlantic Treaty Organization minus Iceland and plus Japan, has a list of products that cannot be sold to the East without approval. But the expertise behind the products is not always so well controlled, and the United States controls some

items that other CoCom members do not, thereby damaging the position of U.S. companies in the world market.

Counterproductive effect feared

"Our concern is that we may be removing U.S. presence without removing U.S. trade," said Joyce Lekas, vice president for communications at the American Electronics Association.

Harry Sello, chairman of the association's International Committee, agrees. "Unilateral rules are the big danger," he says. "If U.S. firms, for example, were kept from exporting CMOS technology, which the Japanese and the French have, then they'd get all the business, and the technology would still fall into the wrong hands. Furthermore, those who export get stronger, so the U.S. will fall behind in both present and future business. You lose immediate business, market share, and your technological lead."

One news report connected the recent purchase by Hewlett-Packard Co., Palo Alto, Calif., of 64-K random-access-memory technology from Hitachi Denshi Ltd., Tokyo, with a loss of U.S. preeminence in semiconductor manufacturing, but HP's manager of international trade relations, Tom Christiansen, contends that the company bought the technology to extend its in-house production facilities, and not for lack of a U.S. supplier.

Under the current regulations, a similar sale of technology by a U.S. firm to a foreign company might face difficulties. According to a source at TI who asked not to be named, export controls pose a significant problem for companies with foreign subsidiaries, since information cannot flow freely between different parts of the same company.

The problems caused by information controls are exacerbated by the complexity of those in place. Over 100 Munitions Control Newsletters have been published, for example, to amend the ITAR since it was published in 1971. Although many in industry have complained about the content of the regulations, one electronics manufacturing source claims that her company's sole problem with the regulation is trying to keep track of the pieces of paper it is printed on.

How effective are current regulations? That is a question Government officials would rather not get into. One DOD official acknowledges that keeping technology confined to the U.S. for a long time is probably impossible. "The purpose is to make it difficult for the Soviets," he said. "If they can save a ruble by begging, borrowing, or stealing the technology, that's one more ruble they can spend on their own research."

How fast U.S. technology reaches the Soviet Union and is put into practice is difficult to determine. And if determined, it is not always revealed, partly because to do so would uncover sensitive intelligence sources and partly because it would embarrass the agencies responsible for controlling technology transfer.

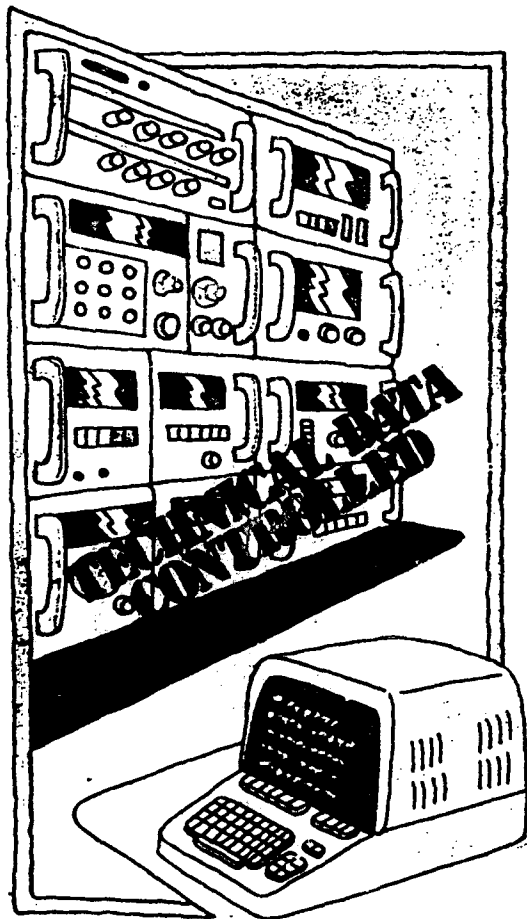
Many industry officials are not much more willing to discuss the effectiveness of export regulations—or, for that matter, any specifics about export control. "We've got to work with the Government," said a manager at one large electronics company. Speaking privately, officials have a number of things to say about the effectiveness and the effects of export controls.

"It's a tremendous bind," said the same manager about controls on information in the arms regulations. "Even if you just publish a block diagram, your lawyers say that it's information."

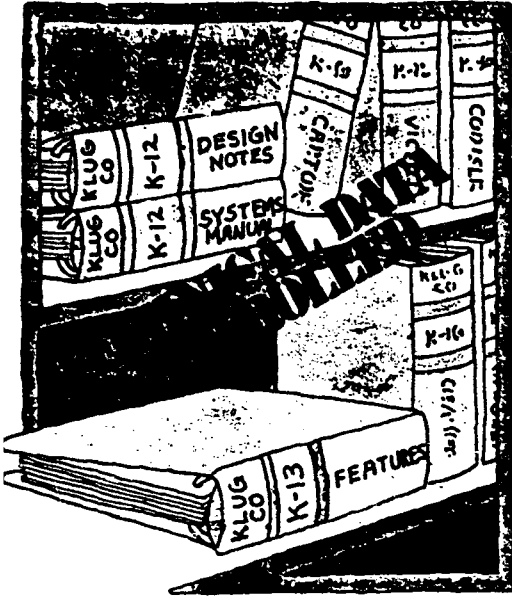
The Government now proposes to tighten technical information controls, so the situation seems unlikely to improve.

The 'dual standard'

University programs are another concern to just about everybody involved: the Government, the universities, and industry. "There is a feeling that a significant amount of technology



(Equipment embodies critical technology.)



(Requires license for dissemination.)

escaped us by 'innocent' transfers between scientists and engineers," said Mr. DeCain at the Commerce Department. He added that such transfers are "not so innocent on the part of the Soviets," but rather are part of "sophisticated acquisition schemes by the Eastern bloc" intended to circumvent U.S. controls on the sale of technology.

He acknowledged that controlling those transfers is a knotty problem. "We recognize that this is an open society, and the Government can't have carte blanche to control ideas." On the other hand, he noted, national security concerns "are designed to protect the same people who may have allowed the technology to escape."

Some industry executives feel that academics have been in a privileged position for a long time and that that privilege may come to an end. Arthur Stern, president of Magnavox Advanced Products and Systems, said: "Frankly, I resent the blindness of academia, which goes by rules made in the 19th century." Mr. Christiansen at Hewlett-Packard said: "There has been a dual standard. Universities have had relatively little Government control of information, while companies have had a great deal."

Mr. Christiansen is worried about possible changes in Government policy. If the Government moves to tighten information controls in universities, he said, "it would constrict the free flow of information between companies and universities: we'd be shooting ourselves in the foot."

One such policy change that Mr. Christiansen fears would be the adoption of the Military Critical Technologies List as the basis for export controls. "The DOD would like to move items on the Commerce Department list to the U.S. munitions list," he said. "Then the DOD would be calling the shots."

As matters now stand, political and foreign-policy questions can sometimes override those of technology transfer. One notorious example is the essentially U.S.-built Kama River truck factory in the Soviet Union, whose equipment was shipped over

DOD objections. Trucks from that factory were used in the Soviet invasion of Afghanistan.

One possible solution to the problems that export controls raise for the U.S. economy is to restrict only the very limited expertise required to produce certain critical defense products and systems. Other technologies and all end products, barring actual arms, would then be exported fairly freely. According to Larry Sumney, director of the DOD's Very High Speed Integrated Circuits (VHSIC) program, what need to be controlled are the step-by-step recipes for producing critical products, such as radiation-hardened chips; the software to produce highly complex chip architectures for signal processing; and keystone equipment used in IC manufacturing. This "critical technologies" approach is now embodied in the DOD's Military Critical Technologies List.

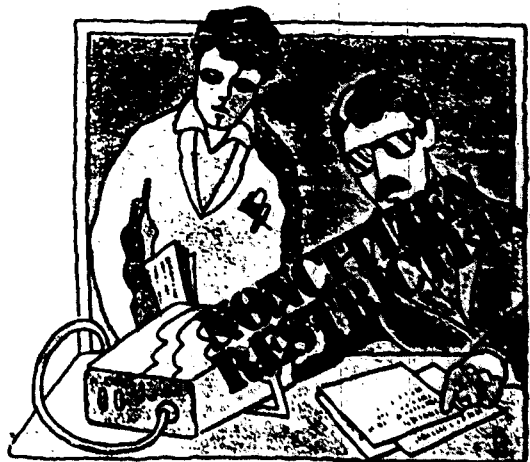
The problem of military secrecy

The list is a classified document containing descriptions of all technologies that defense experts consider essential to modern military systems, from microcircuit design and fabrication to specialized chemical processing and advanced machining. The confidential nature of the list is a problem, since it makes public debate impossible, but to release it would be to give the Soviet Union a "shopping list" of items to target for clandestine acquisition, says one Defense Department source.

He adds that Government's failure to explain adequately the rationale for classifying the list has been a prime cause of many complaints from industry. "There's a big problem of who trusts whom," he concedes. "Each side really should give the other credit for having integrity and smarts, but there's been no appreciation of divergent views."

The current state of the Military Critical Technologies List points up the lack of communication between industry and Government, said Jean Caffiaux, vice president, Government division, of the Electronic Industries Association. Industry commented extensively on a draft of the list last year, he noted, "but those comments were not reflected in the final report."

There has been a good deal of comment on the new list already. "The list of militarily critical technologies is so all-encompassing we wouldn't be able to ship anything," according to Control Data's Mr. Schmidt. There are 700 technologies on



(May not see, discuss, or participate in advance applications.)

the current list, he said, but when his company examined it for criticality, it found only 125 controllable technologies, of which 50 were already proprietary. The problem, claimed Mr. Sello of the American Electronics Association, is defining "criticality." Electronics can be likened to a tree with two branches: military and commercial, he said, asking, "Do you cut off the trunk?"

Questions about critical technologies

In general, however, industry is in favor of the critical technologies approach to controls. When the approach was first

suggested in the Bucy Report, the electronics and aerospace industries set up expert groups in various fields, such as computer networks, IR devices, and high-energy lasers. "It cost industry about \$2 million, all told," according to Mr. Caffiaux. Then, he noted, there was a change of national administrations, and the Institute for Defense Analysis received a contract to put together a new list "with varying degrees of industry involvement."

One cause for concern, he says, is that "the *quid pro quo* isn't *quid-ing*." Control of keystone equipment and technical information is being tightened, but there has been no corresponding relaxation of controls on end-product exports. Industry is being squeezed from both directions.

"We don't expect a one-to-one exchange," Mr. Caffiaux observes, "but so far there's been no relaxation at all."

Emerging technologies, like VLSI design and near-micrometer fabrication processes, pose new problems for industry. Should a manufacturer enter the field and risk losing markets because the process may end up on the Military Critical Technologies List?

"If you don't know what's going to be on the list," said Mr. Sello, "then you have to hold back everything. In many new areas, neither industry nor Government has any firm ideas of what should be controlled."

Mr. Sumney of the Defense Department suggests that the actual controlled technologies in any particular area are quite narrow. In the military's VHSIC program, for example, the areas that will be controlled will be only those with clear-cut military significance, he says, explaining: "We're looking at step-by-step recipes for certain products or processes, such as radiation-hardened ICs or signal-processing circuits."

When asked whether control over very large-scale-integrated architectural software would cover areas in which other countries, such as Japan, are already proficient, Mr. Sumney replied: "They do data processing, not signal processing; they're two very different things." Only in such specialized areas as computed tomography (CT) scanners, seismic monitors, or voice-recognition devices, he said, does industry engage in massive signal processing; and everywhere there is a gap between VHSIC circuits and commercial ones.

The MC68000, a top-line commercial processor, for example, barely meets any VHSIC specifications—it has a clock rate one half the 25-megahertz VHSIC requirement. On the other hand, a speech-synthesizer chip for the talking doll from Fisher-Price, East Aurora, N.Y. [*Spectrum*, January 1981, p. 81] was made by Precision Monolithics Inc., Santa Clara, Calif., to take the same kind of abuse that is required of the military circuits that are the company's primary product.

Some doors still open

Even if the Military Critical Technologies List succeeds in defining critical technologies to the satisfaction of all concerned, however, some transfer of sensitive Western technology to the East is bound to take place. There will still be the problem of clandestine transfer, both by diversion of devices and by reverse engineering of legitimately purchased equipment. More crucially, the list applies only to the United States.

Thus far, there has been very little discussion with any of the other CoCom countries about the list and the possibility of applying it uniformly. "The degree of CoCom cooperation is going to be critical," said Mr. Caffiaux, although he held no very high hopes that such cooperation will be forthcoming. Others expressed a similar view.

"They sign in blood that it won't go [to the USSR]," said Roger Borovoy, general counsel of Intel Corp., Santa Clara, Calif., of technology importers in Western Europe. "But I

Two sets of regulations control information

Technical information is controlled by the United States government under two sets of regulations: the Export Administration Regulations, administered by the Commerce Department, and the International Traffic in Arms Regulations, administered by the State Department. Between them, they cover virtually all areas of technology, from spacecraft to oil-drilling equipment.

Their definitions of what constitutes technical information are quite broad. Under the Export Administration Regulations, the following may be controlled: "Information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization or reconstruction of articles or materials, such as a model, prototype, blueprint or an operating manual, or technical service."

The International Traffic in Arms Regulations cover three categories: "any unclassified information that can be used, or adapted for use, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of arms, ammunition, and implements of war on the U.S. Munitions List, or any technology which advances the state of the art or establishes a new art in an area of significant military applicability in the United States."

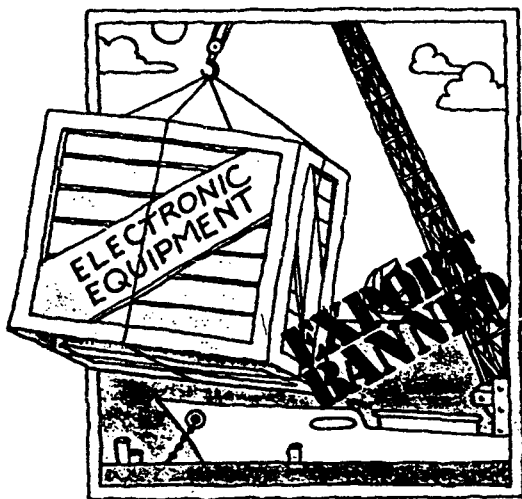
The Department of Defense is generally consulted on license applications because it is assumed that the DOD knows best what items might affect national security.

The language in these regulations is clarified by two lists that enumerate the actual items controlled: the Commodity Control List and U.S. Munitions List. These lists include such diverse items as chemicals, word processors, echo-sounding equipment, missiles, tanks, and combat aircraft. The two lists are supplemented by the Military Critical Technologies List, a classified document that details the design and production expertise required to make items on the commodity and munitions lists. It is expected that the Military Critical Technologies List will eventually be incorporated into the Commodity Control List, although it overlaps both current sets of regulations.

As can be inferred from the position of the U.S. as a leading arms dealer to the world, controls do not mean embargo. Many, if not most, of the items on the munitions and the commodity lists are exported regularly with little difficulty, and some products can be shipped under expediting procedures that do not require licensing of individual shipments.

According to Lloyd Kaufman, director of foreign trade for the Computer and Business Equipment Manufacturers Association, most of whose members' products are controlled under the Export Administration Regulations, "licenses for specific shipments" take anywhere from six months to two years to get. Times tend to fall near the extremes, depending on the sensitivity of the shipment and the current political climate. Embargoes will prevent shipment of even the simplest items, and the spirit of détente has sometimes allowed products to be shipped that would not normally have received a license.

—P.W.



(Keystone equipment will not be licensed for export.)

wouldn't be surprised if the USSR had one of everything," he added. He questions, however, whether the Soviets can always benefit significantly from this. "They can get access to any kind of equipment, but they can't load up a whole fabrication line with it," Mr. Borovoy says.

The Rand Corp., Santa Monica, Calif., issued a report last year with similar conclusions: "The most important question about technology transfer in the long run is whether the receiving side is able to absorb the technology it imports...and to build upon it to generate further technological advances." The report goes on to state that "in certain high-priority areas, notably military, where Soviet technological skills are already high, the Soviets' ability to learn from foreign technology is high.

"But in the lagging areas, where most Soviet imports of foreign technology are concentrated, the Soviets' record in absorbing and learning from it is poor," the Rand report says, concluding: "The most effective barriers against technology transfer are those erected by the Soviets against themselves."

Strong doubts in academia

Meanwhile there are strong doubts in the academic community that militarily critical information can be separated from the total body of engineering and scientific knowledge. "There is no such easy separation in any engineering curriculum intended to be relevant to our national industrial needs and problems," the presidents of the Massachusetts Institute of Technology, the California Institute of Technology, Stanford University, Cornell University, and the University of California system said in a joint letter to the secretaries of commerce, state, and defense last year, attacking statements made in regard to the VHSIC program.

Although a number of options are being explored in the VHSIC program to let a researcher know beforehand of any possible restrictions on the dissemination of results, some in the DOD suggest that the only way to ensure that critical information does not leak is to remove from the universities any research that might lead to specific process or design expertise. One draft memo stated: "While industry needs graduates with hands-on experience, it need not necessarily be with the very latest equip-

ment, nor done in the most elaborate labs."

Needless to say, antagonism has built up between universities and the Government over the issue of information control. Peter Denning, president of the Association for Computing Machinery, voiced his opposition to information controls at the 1982 meeting of the American Association for the Advancement of Science by saying, "If you want to win the Indy 500, you build the fastest car; you don't throw nails on the track."

Although the controversy over controls has at times become quite heated, there are some who think there is not much for academia to worry about. D. Allan Bromley, chairman of the American Association for the Advancement of Science, thinks most of the disagreement between Government and universities is due to misunderstanding and that any actual differences come "only in limited gray areas."

Bohdan Densyk, deputy assistant secretary of commerce for the export administration, also thinks a good deal of the furor over information controls "is due to a misconception of what we're trying to do." He said, "There's actually precious little to be controlled."

What the Government is trying to do, explained Mr. Densyk, is not to "unfairly apply the regulations to just one segment of society," industry, while letting academia operate without any regulations at all. "We're informing many people that the regulations that are in place apply to them," he said. When universities do research with a proprietary technology component to it, they should need an export license to release it. "Our regulations define an exporter as anyone who transmits certain types of data to Communist countries," he noted.

In basic science, however, Mr. Densyk is strongly against any system of controls. Since it is impossible to tell in advance what the results or applications of basic research will be, putting controls on its operation would be foolish, he believes.

To probe further

Reviews of the basic issues involved in technology transfer and export controls are contained in *Technology and East-West Trade*, from the Office of Technology Assessment (1979) and *An analysis of export control on U.S. technology—a DOD perspective* (the "Bucy Report"), from the Defense Science Board (1976). Both papers are available from the U.S. Government Printing Office, Washington, D.C. 20402. A quick overview of some of the problems of export controls on products is contained in "Technology: dichotomous tool," by Thomas G. Lombardo [*Spectrum*, May 1981, p. 51].

Restrictions on academic exchanges and publications have been reported extensively in *Science* (June 27, Aug. 29, and Sept. 12, 1980; June 12, 1981; and Jan. 8 and Feb. 5, 1982) and elsewhere in the popular press. Admiral Inman, deputy director of the Central Intelligence Agency, has taken issue with reports of his views published in *Science* and elsewhere, but the reports nonetheless give good coverage of the controversy.

The subcommittee on Government information and individual rights of the House Committee on Government Operations held hearings March 10 on the new Executive Order for classification, and the subcommittees on oversight and investigations and on science, research, and technology of the House Committee on Science and Technology held hearings March 29 on the general problem of information controls. The text of the new Executive Order on classification is available from the White House publications office; the former order, E.O. 12065, is available from the government printing office.

A report on the *Spectrum* roundtable on information controls and industry will appear in a future issue. ♦

The Communications Revolution
in Politics



Proceedings of
The Academy of
Political Science

Volume 34
Number 4

ISSN 0065-0684

Edited by Gerald Benjamin

New York, 1982

The Invasion of Privacy

CHRISTOPHER H. PYLE

The police state that George Orwell warned against in his novel *1984* arose from three developments indigenous to the twentieth century – the bureaucratic state, the communications revolution, and nuclear war. Orwell wrote of the country of Oceania in *1984*: “There was . . . no way of knowing whether you were being watched at any given moment. . . . It was conceivable that they watched everybody all the time. . . . You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and . . . every movement scrutinized.”¹ Nuclear war and its danger, Orwell feared, would cause militarized states to arm internal security bureaucracies with the technology of surveillance to produce a totalitarian society in which individuals were rendered wholly malleable by the loss of all privacy.

Of the three developments Orwell feared most, the first two have proceeded rapidly and independently since 1948. The third has yet to occur, but its likelihood has also increased insidiously, like a dark cloud that expands each time another nation joins the nuclear club. Because the danger of nuclear war and its attendant social controls grows silently, most citizens of democratic societies seem able to ignore it. Meanwhile, right-wing ideologues who seek to revive domestic surveillance are content to believe that if such a holocaust comes, Big Brother could be safely unleashed for the duration of the crisis.

During the 1970s, when fear of nuclear war with the Communist superpowers dissipated for a while, a series of exposés drastically reduced domestic intelligence in the United States. Continuing this trend, however, has not been easy, and today the suppression of domestic surveillance depends largely on a small band of beleaguered liberals who occupy strategic positions in the House of Representatives. Meanwhile, it is sobering to note that George Bush, a former head of the Central Intelligence Agency (CIA), stands but a heartbeat away from the presidency.

Equally sobering is the extent to which the United States government has ac-

¹ George Orwell, *1984* (New York: Harcourt, Brace & Co., 1949).

quired the technology of surveillance that Orwell could only imagine. Television sets do not spy on citizens as they did in 1984 (although two-way cable systems could be used for this purpose), but other equipment more than fulfills Orwell's expectations. Today, drug smugglers are flushed from the Florida Everglades by helicopter chase teams using infrared sensors that penetrate the thickest foliage to detect people by their body heat. As Orwell anticipated, television cameras patrol buildings and street corners, voice analyzers automate the tedious work of eavesdroppers, computers create Big Brother memories that never forget, and new systems of telecommunications give diverse investigative agencies the capacity to cooperate as never before. Government agencies and private corporations continue to frighten their employees with lie detector tests, while the National Security Agency (NSA), the largest and most secret spy agency in the United States, conducts massive searches of electronic communications without prior permission from the courts.²

As Orwell predicted, ministries of state security have found the new technology for invading privacy irresistible; indeed, they have pioneered its development. For example, much of the early research into hallucinogenic drugs was conducted by the army and the CIA, sometimes with tragic results for unsuspecting human subjects. Computers, which most Americans associate with the socially conscious International Business Machines Corporation, are equally the brainchild of the military intelligence services, which have used their wizardry to breach the privacy of foreign and domestic communications. Today no agency works harder than the NSA to obstruct the dissemination of new mathematical concepts that would permit the development of effective countermeasures to this science of privacy invasion.

Contrary to Orwell's vision, ministries of state security have not been the only, nor always the worst, privacy invaders. Equally intrusive have been television newspeople who descend on tragedy like jackals, ask ghoulish questions, then transmit film of the grieving victims back to blow-dried newscasters who convey it with all of the sighs and clucks of village gossips. However, unlike Orwell's ministers of Truth, today's television jackals concentrate their invasions of privacy most intensely on public officials, an ironic situation that Orwell may not have anticipated but that he surely would have appreciated.

If Orwell did not anticipate the extent to which the communications revolution would strip officials of their privacy, he did foresee their efforts to use television to befuddle people's minds with "newspeak," "doublethink," and other forms of misleading language. Like Orwell's ministers of Truth, United States government spokesmen insist that the armed forces are really part of a "defense" department, that the agency of clandestine warfare is really an "intelligence" agency, and that government lawyers are really part of a "justice" department.

² U.S., Department of Justice, "Report on Inquiry Into CIA Related Electronic Surveillance Activities," reprinted, 1976.

As if this were not enough, officials use the same sort of secrecy ploys used in 1984 to deprive the people of accurate information and to distort history.

Orwell understood that the primary purpose of all official efforts to debase language and undermine the reliability of information is to strip citizens of the capacity and confidence to make moral judgments about the government's use of power. His novel demonstrated in a chilling way that nothing invades privacy more than the manipulation of communications in order to destroy the ability of individuals to know truth and thereby defend themselves against psychological manipulation. But citizens are not the only victims of this manipulation. Politicians also suffer as they come to believe their own propaganda and lose the ability to distinguish between images and reality. Richard Nixon was one such politician, who in the end was destroyed by his blind faith in the power of media manipulation, secrecy, and deception.

In Orwell's world, the communications revolution strengthened the centralizing forces of an authoritarian state. For a while in the early 1970s, it looked as if the United States might suffer a similar fate, as more became known about the use of surveillance technology by J. Edgar Hoover's "Thought Police," Richard Nixon's plumbers, the NSA's eavesdroppers, and the army's political data bankers. But countervailing technologies were also at work. Chief among these was the Xerox machine, which during the 1970s made it easier to copy and leak secret information. The Nixon administration's effort to control the Pentagon Papers, the army's surveillance of civilian politics, and the FBI's programs of dirty tricks against political dissidents were all exposed through the use of Xerox machines. During the 1970s, the army's data banks were destroyed, NSA's watchlists of dissidents were discontinued, the CIA's spying on domestic politics was ended, the FBI's roundup lists were destroyed, the Watergate plumbers were sent to prison, Hoover's "Thought Police" were disbanded, and most police intelligence units were abolished. The defeat of these Orwellian activities, a major victory for political freedom, will not soon be forgotten.

However, the defeat of these activities was only a momentary advance in a much longer war against the forces that Orwell feared. The outcome of this war remains in doubt; there have been as many defeats for privacy as there have been victories. Nowhere is this more evident than in the body of law that defines the right of Americans to the privacy of their communications and the control over the government's collection and use of information about their personal lives.

Communications Privacy

The past three decades have not been kind to the privacy of electronic communications. When Orwell's countdown began, the Supreme Court was unwilling to hold that warrantless electronic searches violated the Fourth Amendment unless the eavesdroppers physically invaded their targets' property. The Court persisted in following the doublethink of Chief Justice William Howard Taft,

who had declared in 1928 that electronic communications were not tangible enough to be seizable, unless, of course, they were seized on a person's property, in which case they were magically transformed and made subject to the Fourth Amendment.

During the 1960s, the Supreme Court finally came to realize how absurd it had been to tie the privacy protected by the Fourth Amendment to the technical laws of trespass. In *Katz v. United States* the Court even declared that the Fourth Amendment protects "persons, not places," thereby establishing a new portable personal right of privacy. What the amendment really protects, the Court seemed to say, are the reasonable expectations of privacy that people should have in certain circumstances.

But this new standard was not without its confusions. Insofar as it liberated the Fourth Amendment from heavy reliance on concepts of ownership and control, the standard constituted a positive gain for individual privacy. However, to the extent that it required proof of the subject's actual expectations, it was regressive, leaving the way open for the government to declare its intent to snoop and thereby eliminate all reasonable expectations of privacy. The Supreme Court, now dominated by Nixon appointees, has come to accept this regressive approach.

When Orwell's warning was first published, section 605 of the federal Communications Act of 1934 clearly forbade the government to "intercept and divulge" the contents of wire communications. Unwilling to accept this restraint or to work to change section 605 by legislation, successive attorneys general simply debased the statute's language. What the law really meant to say, they declared, was that the government could conduct all the nontrespassory wiretaps it desired so long as it did not divulge the contents in court or elsewhere outside the executive branch. In other words, so long as information obtained from eavesdropping was shared only within the government, no harm to privacy would be done.

By this sophistry, the "Justice" Department sought to reduce the Fourth Amendment from a principled guarantee of privacy to a technical, largely pointless, rule of criminal procedure. To these Orwellian "realists," the Bill of Rights was not a body of high moral values but an amoral prediction of what some politically shrewd judge might decide in some future case. Embracing what Oliver Wendell Holmes called the "bad man's theory of the law," they followed the tendency of all lawyers to subordinate their morality to that of their clients. Thus the law of privacy was reduced to what the surveillance agencies could not reasonably expect to get away with.

In 1968, Congress made another attempt to govern wiretapping and bugging. Title III of the Omnibus Crime Control and Safe Streets Act of that year was based on two assumptions: first, that all wiretaps are searches within the meaning of the Fourth Amendment, as the Supreme Court had ruled in *Katz v. United States*; and second, that the Fourth Amendment does not flatly prohibit all general searches of places, even though that was what the Framers had

sought to accomplish. Searches of all telephonic and household communications are constitutional, Congress assumed, so long as they are governed by a reasonable set of authorizations.

Nineteenth-century absolutism about the "sacred privacies of life" was thus replaced with twentieth-century relativism, and the Fourth Amendment reduced to a mere counsel of moderation. Under Title III, criminal investigators are required to obtain a full-fledged judicial warrant before installing a wiretap. After the device is installed, the statute seems to say, investigators are supposed to minimize their intrusion by recording only those messages clearly associated with the purpose of their tap. However, even this requirement has been eviscerated by a 1978 Supreme Court interpretation. If the lawmakers had been serious about minimizing the effects of these general searches, they would have forbidden the investigators to use any information about other criminal activities that they happen to overhear unexpectedly. But the law's draftsmen did not forbid them. Today unsuspected persons who discuss criminal activities on a tapped telephone are as vulnerable to prosecution as the suspect himself. The government can breach their privacy without first establishing probable cause to believe that they are guilty of some criminal activity and that evidence of their crime will be found on the telephone line to be tapped.

In 1984, claims of national security justified all breaches of privacy, for Oceania was in a perpetual state of war with other superpowers. In cold war America, claims of national security have had a similar impact. During the drafting of Title III, national security conservatives quarreled vehemently with civil libertarians over whether the president could constitutionally ignore the statute and authorize the installation of warrantless wiretaps to collect national security intelligence. The conservatives said that the president could, because Article II of the Constitution, or the "concomitants of nationality," gave him an inherent power to ignore restrictive legislation and even the Bill of Rights in order to protect whatever he might deem to be the nation's security. Civil libertarians denied that Article II gave him any such power or that the so-called concomitants of nationality belonged to the president. Accordingly, they refused to accept a provision in the bill that would have acknowledged the concept of inherent executive powers or of a national security exception to the Fourth Amendment. After lengthy debate, Congress finally avoided the issue by expressly disclaiming any legislative intent to resolve the constitutional dispute.

Johnson administration lawyers agreed to the disclaimer. However, when Richard Nixon assumed the presidency, his attorneys insisted that the provision actually constituted positive recognition by Congress that FBI agents could, as the president's lieutenants, ignore the warrant requirements of the Fourth Amendment and Title III whenever they believed that the communications to be invaded might somehow be related to national security. Not surprisingly, the bureau's definition of "national security" was Orwellian in scope.

In 1972, the Supreme Court rejected the Nixon administration's interpretation of the disclaimer. In *United States v. U.S. District Court*, the justices ruled that

there was no inherent power or national security exception to the Fourth Amendment or to Title III for wiretaps directed against domestic political activists who are not agents of a foreign power. In so ruling, the Court separated the Fourth Amendment into its two clauses and suggested that while the reasonableness requirement of the first clause had to govern all electronic searches, the warrant requirement of the second clause might be weakened to facilitate foreign intelligence wiretaps. As in Orwell's *Animal Farm*, all have equal rights under the law, but some are more equal than others.

Two federal courts of appeal subsequently decided that prior judicial warrants for wiretaps directed at alleged foreign agents were not required at all. In the case of H. Rap Brown, a black power advocate, the court even ruled that no prior judicial review of any kind was required by the Fourth Amendment when the purpose was to gather "foreign intelligence." The court declared that the Fourth Amendment's standard of reasonableness could be satisfied in such cases by judicial review at a trial, conveniently ignoring the fact that the purpose of nearly all national security wiretaps is not to collect evidence for a criminal trial but to gather economic and political information and to obtain the means to blackmail people into becoming spies for the United States. The *Brown* decision thus gave the clandestine services of the United States a constitutional license to wiretap at will within the Fifth Circuit, regardless of the consequences to personal privacy.

When the new intelligence committees of the House and Senate undertook to draft the Foreign Intelligence Surveillance Act of 1978, they took notice of these judicial opinions and created a new system of weakened, pro-forma judicial warrants, to be administered by a specially designated national security court. The procedure prescribed by this statute is essentially a travesty of the principle of checks and balances. As a gesture to the probable cause requirement of the Fourth Amendment, the court is directed to decide whether there are grounds to believe that the target of the electronic surveillance is an agent of a foreign power. However, once the court has made this finding, it must accept on faith the executive's certification that the surveillance is rationally and substantially related to the needs of national security. On no account is the court authorized to consider the reasonableness of the proposed search on the basis of the totality of the circumstances—the kind of judgment it presumably would make when assessing an ordinary warrant request.

When this statute was enacted, some of its proponents asserted that it would undermine the appeal of broad executive claims to inherent constitutional authority to ignore both the legislation of Congress and the Fourth Amendment in order to protect the nation's security. Perhaps it will, if such a case ever reaches the Court. Meanwhile, Presidents Ford and Carter refused to renounce the Nixon claim, and President Reagan has affirmed it.

The National Security Agency has also continued its massive interceptions of international telephonic communications to and from the United States. It has done so without any judicial authorization at all—not even a pseudowarrant like that authorized by the 1978 act. NSA ignores all federal wiretap legislation

largely on the theory, which it prudently keeps secret, that legitimate expectations of privacy evaporate as soon as the telephone company decides to bounce conversations off a microwave tower or satellite.³

In 1973, according to the Senate Select Committee on Intelligence, chaired by Senator Frank Church, the NSA had discontinued all of its "watch lists" of United States citizens whose international communications NSA agents had been instructed to intercept. However, there is a document that the Justice Department apparently did not share with the Church committee and that the Reagan administration would now like to recall and reclassify that indicates that the committee was misinformed. Watchlists or their equivalent may still exist, not only to spy on the commercial activities of selected corporations but also to investigate suspected drug smugglers, gunrunners, and terrorists.⁴ Since each of these activities involves criminal activity and none is directly related to the activities of foreign intelligence, military, or diplomatic personnel, it would appear that the NSA is still engaged in the wholesale violation of Fourth Amendment rights.

Thus, despite Orwell's warnings and the exposés of the 1970s, all three branches of the federal government still strive to erode the Fourth Amendment's defenses against electronic spying. The extent of this erosion is most dramatically illustrated by positions taken on the authority of federal agents to conduct burglaries in order to install listening devices for national security purposes. According to the Nixon, Ford, and Reagan administrations, these intrusions may be authorized by the president on his authority alone. The Church committee insisted that a warrant be obtained first but did not object in principle to court-ordered burglaries. Presumably, this means that if one of the government's burglars is surprised and killed by a homeowner, the homeowner would be guilty of murder. Conversely, if the burglar killed the homeowner in the course of a struggle, the killing would not be a crime, because the entry had been authorized by a judge. Such is the Orwellian logic of the "Justice" Department and the legislators who are supposed to oversee it.

Informational Privacy

When Orwell wrote *1984*, intruders still seemed to pose the greatest threat to privacy because privacy was still viewed largely in physical terms. Orwell helped change this view. Big Brother was not only an eavesdropper, a Peeping Tom, and a government spy but also a keeper of records, a mind reader, and a brainwasher. The secret to Big Brother's enormous power was not only physical surveillance; his power was also based on informational control. He knew, or led people to think that he knew, as much about their personal lives as they did themselves. As a result, people lacked the capacity or courage to control Big Brother by limiting what he could know about them.

³ *Ibid.*, pp. 130-42.

⁴ *Ibid.*, pp. 126, 173.

Orwell understood the importance of informational privacy to individual freedom, but since he was primarily concerned with police states, he had less to say about well-meaning officials in liberal democracies who could also destroy privacy with the data they collected to administer social service programs. The idea of informational privacy, in the sense of people having some control over what others know about them, was implicit in the Fourth Amendment's guarantee against unreasonable searches and seizures. Informational privacy was also implicit in the famous 1890 *Harvard Law Review* article by Samuel Warren and Louis Brandeis that launched the tort of privacy against newspaper reporters who publish private information about the lives of private persons. The concept of informational privacy did not win widespread support, however, until the rise of internal security and social service bureaucracies in the post-World War II era, and the development of the new technology of computers and telecommunications.

In the wake of World War II, Orwell was alarmed by the extent to which returning veterans seemed to accept the impersonal, data-hungry bureaucracies of modern socialistic states. By the late 1950s, however, public trust in large organizations had declined substantially, and Americans began to question whether it was wise to entrust so much personal information to unaccountable administrators. This concern was expressed in three stages. The first period of protest occurred in the 1940s and 1950s when civil libertarians questioned the informational practices of the internal security bureaucracies. Unfortunately, knowledge of these files was effectively limited and potential critics were often intimidated.

The second stage occurred in the mid-1960s, when executive-branch officials proposed a computerized national data bank combining personal information about citizens from the records of some twenty social service agencies, including the Departments of Labor, Commerce, Agriculture, and Health, Education, and Welfare. None of the reports recommending this vast records system paid more than perfunctory attention to the concept of informational privacy, and congressional opposition killed the plan outright. Opposition to the national data bank proposal was supplemented by the appearance of an influential body of literature developing the idea of informational privacy.⁵ This literature was reflected in congressional investigations of the era. In 1970, Congress passed its first informational privacy law—the Fair Credit Reporting Act. Although riddled with loopholes, the act gave individuals the right to know the substance of information about them in the files of the giant credit-reporting companies. The act ensured that individuals would be notified when adverse decisions were made on the basis of credit reports, provided for the correction of erroneous information, and required the deletion of outdated facts.

⁵ The most influential works were probably Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967); Arthur R. Miller, *The Assault on Privacy* (Ann Arbor: University of Michigan Press, 1971); and U.S., Department of Health, Education, and Welfare, *Records, Computers, and the Rights of Citizens*, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (Cambridge: MIT Press, 1973).

The third stage of concern was directed against the informational practices of the internal security bureaucracy. In 1971 the Senate Subcommittee on Constitutional Rights, led by Senator Sam J. Ervin, Jr., dismantled the army's program of domestic spying. Ervin built bipartisan support for his investigation and neutralized some of his potential cold war critics by linking the army expose to a more far-reaching inquiry into federal data banks, computers, and the Bill of Rights. Even so, Ervin's political acumen was insufficient to convert Senator James Eastland, the right-wing chairman of the parent Judiciary Committee, and the bill to end army surveillance never reached the Senate floor.

However, the Senate hearings on army surveillance did make it politically easier for Ervin and other members of Congress to investigate the Nixon administration's misuse of confidential tax information and the political surveillance and records systems of other federal agencies, including the FBI, the CIA, and the NSA. The most successful of these investigations was conducted by the Church committee. As a direct result of that investigation, the FBI was forced to discontinue most of its domestic intelligence program, including its roundup lists of dissidents. Hoover's "Thought Police" were retired out of the bureau or reassigned to more legitimate areas of investigation.

In 1974, Senator Ervin's Subcommittee on Constitutional Rights launched the first major effort to regulate criminal justice data banks. That effort also failed to produce legislation, but the subcommittee did persuade Congress to pass the Privacy Act of 1974. The act was a product of the Watergate controversy and the consequent need of politicians of both parties to reaffirm their allegiance to the concept of privacy before the fall elections. Two alternatives were available to the legislators. They could attempt a comprehensive statute purporting to regulate all (or most) data banks of personal information, or they could draft narrower, more detailed legislation in such issue areas as banking, insurance, and arrest records. Prudence, respectful of complexity, recommended the issue-by-issue approach, while politics, driven by urgency, insisted on an omnibus statute. Thus, while work on a criminal justice data-bank bill was bogged down in a morass of technical detail, advocates of the privacy legislation took the high road, bypassed all nongovernmental and state data banks, avoided most investigative and intelligence files, and came up with an omnibus law that most members could endorse.

The result was less a privacy bill (in the sense of a law declaring what should be private or confidential) than a code of fair information practices grounded in theories of due process of law. Still, the Privacy Act established eight important principles that may someday take on constitutional significance. First, the act forbids the government to maintain any secret data banks of personal information about individuals. Second, it grants individuals the right to see and copy information about themselves, except when the information is expressly exempted from disclosure, as in the case of investigative and national security files. Third, it gives individuals the right to correct and amend their files. Fourth, it prohibits agencies from collecting any personal information that is not relevant and necessary to the accomplishment of a lawful purpose. Thus the revival of

domestic intelligence files is arguably forbidden. Fifth, the law directs agencies to limit the extent to which information collected for one purpose can be shared with other agencies and used for other purposes. Sixth, it restricts the power of agencies to disclose confidential information to outsiders without the subject's consent. Seventh, it charges agencies with an affirmative duty to see that personal information that they keep on individuals remains necessary, lawful, accurate, and up-to-date. Finally, the act makes it possible for individuals to hold agencies accountable for their handling of personal information, if necessary by suing them for damages or by initiating criminal prosecutions for egregious misconduct.

Unfortunately, the Supreme Court has been far less sensitive than Congress to the dangers posed by the new technology for handling personal information. Indeed, President Nixon's appointees have been downright Orwellian. For example, in 1972, they refused to allow the innocent subjects of the army's computerized political data banks to challenge the constitutionality of that surveillance. The chilling effect on political activists caused by the existence of the files was not enough. Justice Burger ruled, to give the plaintiffs standing to sue. They had to prove that the surveillance had caused them more tangible injuries, like the loss of jobs, mortgages, or reputation. Of course, they could not prove such injuries unless they could learn what the army had done with the files, but the Nixon appointees refused to allow the plaintiffs to examine the records. Burger's ruling was a classic Catch-22 decision—"doublethink" at its best—and it effectively immunized the internal security data banks from constitutional challenge in court.

The most Orwellian of recent Supreme Court opinions have flatly refused to recognize a constitutional right of informational privacy. According to the Nixon justices, persons assume the risk, when they entrust their checks to a bank, that its officers will make copies of those checks available to government investigators on demand, even without telling them. Similarly, the justices have ruled that while persons have a legitimate right to expect that the government will not listen to their telephone calls without first obtaining a warrant, they do not have a right to expect that the the government will get a warrant before installing "pen registers," which record the numbers dialed.

There are numerous indications that the courts are waiting for Congress to exercise leadership in the development of informational rights of privacy. However, Congress has not made much progress in recent years. In 1978, the legislature did succeed in forbidding schools that received federal funds to release a student's files without the student's consent (or the consent of a parent when the student is not yet eighteen years old), and also gave students the right to see and submit corrections to their files. Congress also passed a Right to Financial Privacy Act in 1978; but federal investigative agencies defeated provisions that would have required them to obtain warrants before searching bank records. Other records systems, including insurance files, medical records, and personal records in the possession of private corporations, have escaped federal privacy legislation altogether.

Perhaps the greatest failure to expand informational privacy has occurred in the realm of arrest records, where automation has grown dramatically in the past decade. The problem posed by these files is best stated by William R. Coons, a former convict who served time at New York's Attica Correctional Facility: "Once you have a 'jacket'—a dossier with all the past details of your life, all the detrimental ones they can put together, that is—you are a criminal. The jacket does not disappear; it grows fat and follows you around wherever you go. Some day this sentence you are serving will chronologically run out, but society does not forgive, it keeps tabs. . . ." In 1971, when these words were written, most criminal history records were still in file folders, and most communications among police departments were by telephone or mail. Today, many states and the federal government keep track of criminal suspects by computers and exchange these records by teletype machines.

The new technology has made law enforcement among thousands of governmental units more efficient, but it has also created a new source of systematic injustice—the "records prison." Criminals are not the only persons with criminal records. A quarter of all Americans have been arrested at one time or another for nontraffic offenses. About half of all males and 12 percent of all females will be accused of a nontraffic offense sometime in their lives. For black men living in cities, there is a 90 percent chance of being arrested at some time. And persons who have been arrested once face increased odds of being arrested again, particularly as police departments install computer terminals in squad cars.

Today, the criminal history, or "rap sheet," of the accused is central to every stage of the criminal justice process except the trial, and 90 percent of all cases are concluded without a trial. Contrary to popular impressions, traditional concepts of due process—such as the presumption of innocence, the right to confront witnesses, and the right to open proceedings—no longer characterize the criminal justice process. The system today is largely administrative, as in Orwell's Oceania. The most important decisions are made outside of court, pursuant to a presumption of guilt, without an adversary hearing and often without representation of counsel. Decisions involving prearrest investigations, postarrest investigations, plea-bargaining, sentencing, and corrections all are heavily influenced by the contents of the individual's file. The rules governing these files thus determine, to a considerable extent, the integrity of the criminal justice system and the fate of the accused.

The "records prison" created by criminal histories is not confined to the criminal justice system. Arrest and conviction records are also used extensively in employment, licensing, and even public-housing decisions, often with a disproportionate impact on black Americans. One study in the early 1970s found that 75 percent of the employment agencies in the New York City area would not accept applicants with arrest records. Convictions are an even stronger barrier to employment. State laws deny former convicts licenses to be

* William R. Coons, "An Attica Graduate Tells His Story," *New York Times Magazine*, October 10, 1971, p. 20.

lawyers, teachers, masseurs, fortune tellers, junk dealers, dry cleaners, barbers, plumbers, and taxi drivers.

But the unforgiving nature of the criminal records system is only part of the problem. The other part involves the inaccuracy of the records themselves. A recent inventory of state criminal history files found one state in which 70 percent of the files were inaccurate, incomplete, or misleading. Thus the "records prisons" into which many Americans are being cast are not even of their own making.

Congress, after failing in 1975 to draft a statute that would regulate all state and federal criminal histories systems, consigned the matter to its Office of Technology Assessment (OTA) for further study. The more OTA learned about the patterns of crime and the movement of criminals, the less need there appeared to be for a centralized system of criminal history records. Despite the great mobility of American society, most violent crime remains highly localized. Thus, there is less apparent need for the kind of national system that could produce Orwellian results. However, while the need for more accurate, complete, relevant, and timely records remains at all levels, the political system most capable of legislating reforms is still stymied by jurisdictional wrangles, budgetary constraints, and the antiprivacy demands of companies and professions that are determined to use criminal history files to exclude former suspects and convicts from employment.

Conclusion

It is tempting, after reviewing the weak state of informational privacy today, to blame the communications revolution for the present situation. However, the temptation should be resisted. Technology can create new opportunities for privacy invasion, manipulation, and control, but it does not by itself create the structure of power that commits those abuses. The worst abuses associated with privacy invasions in recent years—the FBI's secret programs of covert action against political dissidents—were committed by agents who used information stored in file cabinets.

The most massive invasions of communications privacy—the NSA's computerized eavesdropping on telephonic communications—are clearly a product of technological developments. However, the technology that the NSA uses against privacy could be easily turned against the eavesdroppers if the public knowledge and political will were there. Technology can also improve the quality of arrest records. Computers can be programmed to block the distribution of incomplete records and to purge outdated information systematically. The political challenge, as Orwell would surely agree, is to wrest these systems from the exclusive control of professionals and technocrats, and to restrain these professionals and technocrats to think in larger, more humane terms.

Appeals Court Upholds CIA Censorship of Article

POST, OCT. 5, 1983

By Al Kamen
Washington Post Staff Writer

A panel of the U.S. Court of Appeals for the District of Columbia Circuit yesterday upheld the CIA's censorship system because it "protects critical national interests," the court said.

Circuit Judge Patricia M. Wald, writing for a unanimous three-judge panel, said the CIA acted properly in censoring portions of a 1981 article written by former CIA officer Ralph W. McGehee.

McGehee, who left the agency in 1977, wrote an article for *The Nation* magazine on the agency and El Salvador. It appeared in April, 1981, after the CIA censored portions and deleted them.

The agency contended that the censored portions, involving countries where the CIA had bases and details of a CIA operation in Indonesia, would disclose intelligence methods and identify sources.

In its ruling, the panel said the CIA's system of classifying documents as top secret, secret and confidential was constitutional "when balanced against the First Amendment interests in public disclosure of former agents' writings."

Wald said that courts should "satisfy themselves from the record, [in secret hearings] or otherwise, that the CIA in fact had good reason" to censor the information.

But in this case, Wald wrote, the agency properly classified and censored the information.

The court also ruled in two cases

involving the Environmental Protection Agency. In one, a three-judge panel unanimously rejected claims from auto makers that EPA abused its discretion under the Clean Air Act in approving tests to check vehicle exhaust emissions.

Circuit Judge George E. MacKinnon, writing for the panel, rejected claims by the manufacturers that the tests were unreliable. Manufacturers must guarantee that properly tuned cars and light trucks will pass emissions tests for five years or 50,000 miles or pay for whatever needs to be done to bring them into compliance.

The emissions tests are now used in 16 states, including Virginia and the District of Columbia. Maryland and several other states plan to begin using the tests within the next year, according to EPA officials.

In the second case—a consolidation of a dozen suits involving the Clean Water Act—several corporations appealed U.S. District Court Judge Thomas A. Flannery's decision last year involving a settlement between the EPA and the Natural Resources Defense Council.

The companies argued that the agreement, which required the EPA to issue standards and limits on the amount of 65 chemicals various companies could discharge, improperly infringed on the EPA administrator's discretion in making decisions on how to implement the Clean Water Act.

A three-judge panel, in a 2-to-1 decision, upheld Flannery's ruling.



BULLETIN

September, 1982

Issue 1

National Security and Scientific Freedom

During the AAAS Annual Meeting in January 1982, Admiral Bobby Inman (former Deputy Director of the Central Intelligence Agency) stated that "There is an overlap between technical information and national security which inevitably produces tension. This tension results from the scientist's desire for unconstrained research and publication on the one hand, and the federal government's need to protect certain information from potential foreign adversaries who might use that information against this nation. Both are powerful forces, thus it should not be a surprise that finding a workable and just balance between them is quite difficult. But finding this balance is essential, for we must simultaneously protect the nation and protect the individual rights of scientists both as academicians and citizens."

Admiral Inman then proposed that certain kinds of unclassified scientific and technical information should be protected from publication and exchange within the scientific community, because of the adverse impacts on national security resulting from such open communication.

Admiral Inman's remarks brought to the public limelight a Federal Government proposal to expand controls over unclassified research that had been developing at the Departments of Defense and Commerce and in the intelligence community for some time. These proposals for stronger controls in the publication of unclassified information have triggered a storm of protest within the universities and scientific and engineering groups. Industrial officials have also expressed concern about the extent to which these controls would affect their own activities. On the same day that Admiral Inman presented his remarks, the AAAS Council unanimously adopted a resolution stating that "Whereas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and the scientific process, . . . the AAAS opposes governmental restrictions on the dissemination, exchange, or availability of unclassified knowledge."

Since January, arguments in favor of and opposed to stronger controls on sensitive but unclassified scientific and technical information have appeared in diverse arenas, including the popular media, the scientific press, trade journals, congressional hearings, interagency meetings, and professional society conferences. However, apart from the new Executive Order on the classification authority of the

President, no new regulations or legislation have been enacted to implement stronger controls on unclassified information. The "interim" policy on technology transfer adopted by the Defense Department in 1977 also has not been changed.

The debate about restrictions on scientific communication has been closely watched by the Committee on Scientific Freedom and Responsibility of the American Association for the Advancement of Science. The Committee is chartered by the AAAS to monitor the policies and actions of the government of the United States, the governments of other nations, and private organizations, that circumscribe or restrict the freedom of scientists or restrict the ability of scientists to exercise their professional responsibilities as scientists.

During its April 1982 meeting, the Committee members expressed concern that the development of "the workable and just balance" sought by Admiral Inman was seriously hampered by the absence of a public forum to explore the issues and assumptions proposed by those who favored stronger national security controls or those who opposed further restrictions on the open communication processes in science and technology. No single group represents all the participants or activities associated with the debate over this issue. As a result, those who are concerned about the problem, but who are unable to keep in touch with new developments, are often unable to identify where or when important decisions related to this issue will be made.

The Committee suggested that in order to keep interested persons informed about the evolution of new information control policies, it would be useful to publish an occasional report summarizing the selected government and private sector activities which relate to this issue.

This is the genesis of *The CSFR Bulletin*. It will serve as a forum for discussion of new policy developments in the national security/scientific freedom arena, and on occasion Committee members and others will review selected reports for the general reader. It will highlight upcoming meetings and deadlines, and will suggest references for further information.

This initial issue of *The CSFR Bulletin* will be mailed to about 100 persons who have previously expressed interest in this topic. We welcome your comments on the reports described here, and we offer these pages as an opportunity for expressing your personal views in future issues. □

A Defense Science Board Report

Are the Proposed Controls Worth the Price?

In January 1982, the Department of Defense (DOD) published a report on the relationship of the university community to the DOD. The report was written by a Task Force of the Defense Science Board under the chairmanship of Dr. Ivan Bennett. Prepared at the request of the House Committee on the Armed Services, it is a comprehensive study encompassing university attitudes, contracting procedures, finances, manpower, foreign nationals and the control of exports of sensitive research results especially to the Soviet Union.

The principal recommendations of the Task Force call for increased funding of academic research, equipment, facilities, fellowships and educational support and for simplification of contracting procedures. The Task Force also called for the Secretary of Defense to encourage other agencies to strengthen language and area support programs. Finally, it proposes a system of controlling the release of unclassified research results which are determined to be sensitive to an item on the Military Critical Technologies List. This is the subject of the remainder of this report.

The Task Force's analysis, in abbreviated form, is that in the last several years problems have arisen in the conduct of university research with respect to the handling of sensitive unclassified defense information because of three factors.

First, the nature of military technology is changing. Whereas research on military specific technology was once somewhat contained in industry and government laboratories and a few universities, all high technology today, with few exceptions, has military impact. The dual

use of technology for military and commercial purposes is becoming the standard.

Second, the interests of university researchers in changing and applied science is receiving more attention. Recent developments in genetic engineering are referred to as an example of this trend toward applied rather than basic research.

Third, the table of contents of the Military Critical Technologies List (MCTL), which first appeared in the Federal Register in October 1981, lists the technologies DOD believes should be subject to export control. While details of the MCTL remain classified, they are believed to be more general than either the International Trade in Arms Regulations (ITAR) or the Export Administration Regulations (EAR) concepts in terms of technology know-how and are more oriented to manufacturing processes.

The Task Force acknowledges that there has been little guidance to the academic community on what technologies are sensitive and why they should be guarded. The fact that the MCTL is classified limits its value as a source of guidance. The report recognizes that vigorous efforts to control research could damage the very research activity it is seeking to revitalize. Yet, not to make some effort could result in loss of militarily critical technology.

DOD Guidelines Proposed

The solution proposed is that DOD guidelines be part of DOD contracts for unclassified university research. Since university research that is militarily critical is for the most part DOD funded, these guidelines would be prepared by

Calendar

The *National Academy of Sciences Panel on Scientific Communication and National Security* (chaired by Dr. Dale Corson of Cornell University) plans to publish an interim report in late September 1982. The report will include an assessment of the extent to which unrestricted academic research is a source of harm to U.S. national security, and preliminary recommendations from the panel. The House Science and Technology Committee, and possibly others, plan to hold hearings on the NAS report when it has been released. (For further information contact the NAS Panel's Executive Director, Larry McCray, phone 202/334-2243.)

The *Office of the Defense UnderSecretary for Research and Engineering* is reviewing a third edition of the Military Critical Technologies List (MCWL) which will serve as a guide to "sensitive" technologies for the new export control and munitions control regulations. A classified version of the MCTL will be prepared in the fall; an unclassified version is under consideration. (Contact Col. George Williams, phone 202/694-8667.)

Bohdan Denysyk, Deputy Assistant Secretary of Export Administration in the Commerce Department, has announced that revised regulations affecting the export of sensitive technologies under the *Export Control Act* will be published for comment in the fall of 1982. His office is currently preparing preliminary drafts of the proposed regulations for inter-agency comment. Comments from academic groups on the preliminary drafts are being solicited by Commerce through the National Science Foundation. (Contact Dan Hoydysh at Commerce, phone 202/466-5030.)

The *Department of Defense/University Forum* (co-chaired by Richard De Lauer, Defense UnderSecretary for Research and Engineering and Donald Kennedy, President of Stanford University) will hold its second meeting on 26 October 1982. The Forum established three working groups during its first meeting in the spring. These will address export controls, engineering and science education, and foreign language and area studies. (For further information contact Jack Crowley at the Association of American Universities, phone 202/466-5030.)

DOD's research and development experts in appropriate consultation with the universities. In general, they would deal with manufacturing and process-oriented research rather than basic research. They would provide for pre-release review, subject to a 30- to 60-day deadline for the review. The DOD contract officer would determine whether the information or data relates to one or more of the thousands of critical elements specified under the 620 technology titles in the MCTL. The contract officer would also establish a DOD position as to whether ITAR and/or EAR are applicable. If so, a researcher would presumably apply to the State Department (ITAR) or the Department of Commerce (EAR) for a formal license to proceed with release of the information. The report does not address those situations in which research is related to an MCTL item but is not deemed to be subject to ITAR or EAR.

In the second phase of this effort to control the release of militarily critical information, DOD encourages other agencies to use similar funding guidelines for university research. In the third phase, DOD would seek to extend the system to industry funded research and to research funded internally by universities.

Sensitive to the argument that information flow restrictions violate academic freedom and will damage the research process itself, the report states that DOD is not seeking "to restrict the flow of all scientific information directly or indirectly related to military capability. . . . The Department of Defense is assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research."

Restrictions on Foreign Students

With respect to foreign nationals, DOD contracts ordinarily exclude students from communist countries from having access to DOD funded projects and seek to exclude foreign students from participating in advanced research considered highly sensitive or specifically related to the development of militarily critical technologies. The Task Force suggests additional flexibility when the possibility of developing ITAR controlled data has been established. In such cases, principal investigators could be asked to assign only citizens or immigrant aliens to program elements likely to produce such data and to limit access to the remainder of the program to foreign nationals who have declared that they do not intend to expatriate their acquired knowledge.

Peer review mechanisms are referred to in the report in the form of ad hoc committees established by discipline or within the framework of scientific societies, as of possible use in controlling non-federally financed research.

That, in essence, is the Defense Science Board proposal. It proceeds from the premise that knowledge and technology transfer from the U.S. universities to the Soviet Union have been used to advance Soviet weaponry and other military technology resulting in unacceptable adverse impacts on U.S. national security. Proceeding from that premise, the report makes a case for imposing controls over university research.

Freedom of Communication will Suffer

Controls, however, exact a price. In this case, the price would be impairment of the freedom of communication which has been an integral part of the atmosphere in which American science has flourished. Knowledge which does not enter the scientific market place is denied the benefit of

peer review and cannot become the base for further advancing such knowledge.

The question then is whether the benefit is worth the price. That there will be a price is recognized by the report, but it is minimized by the argument that only manufacturing and process-oriented research (in contrast to basic research) are of concern. The report asserts that DOD is "assiduously" rejecting controls on development or dissemination of the fruits of basic research by emphasizing that the guidelines would be prepared in consultation with the universities and by drawing attention to the analogy of the protections provided information developed by industrially funded university research. The Department of Defense Research and Engineering (DDRJE) advocates that basic research (6.1 funds in DOD terminology) be outside the scope of this program, except for a few especially sensitive subjects. However, no decision has yet been made.

Nevertheless, disturbing questions remain. For example, if despite this control system, sensitive unclassified information of military value is still found to move to the Soviet Union, are stricter controls then to be imposed?

Since many, if not most, of the DOD's concerns are also being pursued by researchers in other developed countries, how is the publication or discussion of the results of foreign researchers to be approached?

What will be the qualifications and qualities of the officials who will administer the controls and make the decisions? Will they be government officials who understand the nature of academic research and are themselves experienced researchers or officials whose perspective reflects their responsibilities for dealing with the tensions of United States relations with the Soviet Union?

Even if a reasonable and workable program could be installed at DOD, would it be possible to maintain common standards when the program is extended to the rest of the government and to industry? For that matter, can the Department of the Army, Navy and Air Force be brought to adhere to common DOD standards?

University Self-administration

Perhaps the most serious of all the potential consequences of installing the proposed DOD system is not that the bureaucracies would administer it with a heavy and insensitive hand, but that the universities would begin to self-administer the program. They might well begin to anticipate the government's wishes and avoid actions which they think might give rise to conflict or argument. It is one thing to subject an invitation to a foreign researcher to government review. It is quite another not to issue the invitation at all for fear the review would raise problems or be negative. Without intent or design, academic freedom in scientific research might undergo significant change in form and content.

Many other specific and general questions are raised by the proposals of the Defense Science Board. At this time one set of guidelines has been developed and another is near completion. However, neither has been put into force. Before the end of the year there are plans to issue interim guidelines which will apply to the entire MCTL technology base. Therefore, specific guidelines will be issued as they are ready; it is likely that the DOD procedures will be in place before the questions they raise are adequately addressed by the universities. The least that can be said is that the DOD proposals deserve more earlier attention than they appear to have been receiving.

Herman Pollack, George Washington University

Massachusetts Institute of Technology



Interim Report of the Committee on the Changing Nature of Information

March 9, 1983

TABLE OF CONTENTS

Preface	4.3 The Export Administration Act of 1979 (EAR)
1. Summary	4.4 Executive Order 12333 on National Security Information
2. Introduction	4.5 Contract Terms and the Immigration and Nationality Act
2. Historical Background	4.6 Interpretation and Conclusions
2.1 The DES Standard	5. Issues
2.2 Public Key Cryptosystems and the RSA Algorithm	5.1 Critical Technologies
2.3 The Davis Security Order	5.2 The Problems of Technology Export
2.4 The ACE Public Cryptography Study Group	5.3 The Problems of Constrained Research
2.5 The NSF Policy Changes	6. Recommended MIT Policy
2.6 Very Large Scale Integrated Circuit Research	6.1 Introduction
2.7 The Report of the Defense Science Board Task Force	6.2 Recommended MIT Policy
2.8 The Cannon Report	6.3 Relationship of MIT Policy and Cannon Report
3. The Legal Framework	Appendices
3.1 Introduction	A. Committee Membership
3.2 The Arms Control and Export Act of 1976 (ITAR)	B. The Five Presidents Letter

PREFACE

There is little question that we are well into an Information Revolution which may affect the world as profoundly as the industrial revolution of the nineteenth century. The associated geopolitical and geo-commercial developments have already begun to alter the traditional, war, and hence the value, of information in our society. The consequences of these changes are now being felt in the university as the Government seeks to control the dissemination of research results in cryptography and very large scale integration (VLSI) of circuits, and to restrict the participation of foreign scholars in U.S. university research activities.

The forerunners of these developments led the Provost of MIT in October 1980 to establish the MIT Committee on the Changing Nature of Information under the following charge:

The changing nature of information results from the rapid growth of information processing and communications, and in particular of intercommunicating geographically distributed computer systems, and is likely to necessitate new legal, social, and economic approaches for dealing with information. Examples include: (1) privacy and protection criteria that may have to be met before computer data banks become interconnected; (2) the related recent issue of university cryptography research, which has important civilian and military repercussions; (3) export control of information; and (4) the consideration of new laws to deal with the changing nature of information. The committee is specifically charged to identify major issues and questions related to the changing nature of information, and to suggest what steps we should take in order to better inform ourselves and others of these issues and their consequences; and to recommend a range of positions for MIT.

The above charge was extended in May 1981 as follows:

The Committee should also address the questions of technology export and participation of foreign students and faculty in research. The context for these questions and the focus of the Committee recommendations should be MIT's research in very large scale integration (VLSI) of solid state circuits, although it should be anticipated that such questions may arise in other research areas as well.

This revised report of the Committee on the Changing Nature of Information has been written to inform the members of the MIT community about relevant issues, and recommended policies along the principal directions of the above charge.

For the Committee,

M.L. Dertouzos, Chairman

1. SUMMARY

This is an interim report of The Committee on the Changing Nature of Information, which was formed by the MIT Provost in October 1980 in order to identify major issues and recommend policies in cryptography and VLSI research. These specific research areas reflect an emerging broader conflict between (1) governmental desires to control the flow of information deemed important to the national security and the international commercial interests of the U.S., and (2) academic desires to engage freely in research and to communicate without restrictions the fruits of that research.

The historical background relevant to these issues is as follows:

- In the mid-1970's a conflict emerged between civilian and military cryptography needs through the development of the National Bureau of Standards Data Encryption Standard (DES) which was criticized as being sufficiently difficult to prevent commercial interception but not so difficult as to prevent governmental interception.
- In 1977 researchers at Stanford and MIT discovered, and publicly disclosed, a "foolproof" encryption scheme whose publication was criticized as possibly violating regulations (International Traffic and Arms Regulations) that control the export of munitions and related technology. Upon determination by our attorneys that these laws were confusing, we continued our research in this area and volunteered to adopt a policy under which papers in cryptography are sent to the National Security Agency (NSA) for their information at the same time that they are sent to our close technical colleagues for comment.
- In 1978 Professor George David of the University of Wisconsin-Milwaukee, who applied for a patent on a cryptographic scheme, was ordered by the Department of Commerce not to discuss or write about his invention. Although the secrecy order was lifted shortly thereafter, it increased the existing controversy.
- In 1980 at the request of the NSA, the American Council on Education (ACE) established the Public Cryptography Study Group to recommend procedures aimed at easing cryptography research conflicts. The committee developed a set of recommendations based on voluntary prior restraint. At MIT, we reacted negatively to some of these recommendations and declared our preference for our own approach for reasons which are discussed in Section 3.4.
- In 1981 the National Science Foundation (NSF) amended its policies on research grants, requiring prior restraint on "potentially classifiable research results." MIT, objecting to this language, negotiated with NSF more acceptable language consistent with the relevant Executive Order on classification whereby such prior restraint is invoked only in those extremely rare instances when research results are "believed to require classification."
- In 1980 the Department of Defense (DOD) established a research program in very high speed integrated circuits (VHSIC) capable of high speed operation in thermally and radioactively hot environments. Concerned about leaks of this new technology to foreign nations, governmental representatives attempted to restrict publication results and the access of foreign scholars to U.S. university research, under Commerce's Export Administration Regulations (EAR). In a letter (Appendix B) to the Secretaries of Commerce, Defense and State, five university presidents, including

MIT's Dr. Paul E. Gray, explained how such restrictions would harm one of the principal technological assets of this nation—university research.

- In January 1982 the "Report of the Defense Science Board Task Force on University Responsiveness to National Security Requirements" was submitted to the Secretary of Defense. This report addressed several issues associated with DOD sponsorship of university research and may have been the first to emphasize the use of the research contract as the focal point for controlling the flow of scientific information.

- In September 1982 a special panel of the National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine issued its report on "Scientific Communication and National Security." This report, widely known as the Carson Report, sets forth a set of principles aimed at resolving the complex issue that is the subject of our own report, i.e., the conflict between national objectives of scientific communication and national security. We find ourselves in agreement with the principles of the Carson Report but have certain concerns about the way in which these principles may be interpreted or implemented.

The legal framework for governmental control on technological information includes: (1) The International Traffic in Arms Regulations (ITAR) administered by the Department of State; (2) the Export Administration Regulations (EAR) administered by the Department of Commerce; and (3) Executive Order 12356 on national security. The first two forbid the export without licenses of munitions, commodities, and technical data identified by corresponding lists and associated interpretive instruments. The Executive Order provides for the classification of information, including the results of federally funded research, if disclosure presents a danger to national security. These regulations are complex, bewildering and unclear in their application to scientific and technological research. Moreover, they appear to be impractical for controlling university research. Nevertheless they carry substantial penalties that could have a chilling effect on university research and would result in considerable turmoil if they were to be invoked. Beyond the above three regulations, the Government may decide to use the contractual mechanism as a means for controlling technology transfer: A proposal toward that end is currently under consideration by the Department of Defense. Another potential governmental control stems from the Immigration and Nationality Act which could be used to refuse admission or deport foreign scholars from U.S. research activities.

The issues that emerge from this conflict generally concern research that has basic and applied components, dual civilian and military uses, and commercial repercussions on international competition. Such research is pursued by universities because, so in the case of VLSI, it is inextricably linked to forefront technologies that underlie established academic disciplines or, as in the case of cryptography, it leads to technologies that are believed to be essential to society in the future.

The Government wishes to control technology leaks in these basic research areas because such leaks may involve national security and economic losses associated with international competition. Such controls generally take the form of prior restraint on publication of research results and restriction of access to U.S. university research by foreign scholars.

Universities object to such controls because they are ineffective, because they impact adversely on the education and training of future scientists and engineers, and because they generally run counter to present approaches for

carrying out academic research. Moreover, constraints on the access of foreign scholars to U.S. university research reduce the size and quality of the U.S. research workforce and are impossible to enforce without creating a discriminatory climate that is incompatible with university traditions. Ultimately, such constraints are perceived by us as reducing our overall scientific and technological leadership and of questionable effectiveness in meeting the Government's objectives.

To strike a balance between the concerns on both sides of this conflict, our Committee recommends a MIT policy which is summarized in Section 6.2 of this report.

2. INTRODUCTION

All of the issues addressed by this report center on the dissemination of information in the context of university instruction and research. Broadly viewed, the conflict that emerges results from the Government's desire to control the flow of information which is deemed important to national security, and the university's desire to pursue freely the generation of new knowledge. To date, MIT has experienced this conflict primarily in two research areas—cryptography, and very large scale integration of solid state circuits.

The factors that have led to this conflict are: (1) the rapidly evolving technology of information processing and communications; (2) the increasing possibilities for dual use of this technology for military and civilian purposes; (3) a decreasing distinction between basic and applied research; and (4) an increased perception that U.S. technology is being exported, thereby weakening this country politically and economically on a world-wide basis.

Our Committee (Appendix A) arrived at its current conclusions through discussions at 23 meetings. Invited guests who were kind enough to express their views before our Committee were Dr. Robert E. Kahn, Director of the Information Processing Techniques Office at the Defense Advanced Research Projects Agency; Dr. Frank Press, President of the National Academy of Sciences; and Mr. Howard Rosenbom, Deputy Director of the National Security Agency. In addition, Committee members attended meetings and contract negotiations with government officials at the NSF, the NSA, and the DOD. Legal counsel was retained in Boston (Mr. Robert Sullivan of Herrick and Smith) and in Washington (Mr. Carl Faldutson of Palomar Corporation) to analyze the complex laws and regulations surrounding the issues of concern.

This report contains four main sections. A historical survey of developments, especially as they have affected MIT, is presented first (Section 3) in order to explain how we became involved with the relevant issues. Section 4 discusses the framework of current laws and regulations that deal with controls on technological data. Section 5 strives to analyze the crucial issues that emerge in this controversy, and Section 6 presents our Committee's recommendations for an appropriate MIT policy.

2. HISTORICAL BACKGROUND

2.1 The DES Standard

The public concern over cryptology began in the mid-1970s in connection with the development of the Data Encryption Standard (DES). This standard, set forth by the National Bureau of Standards (NBS) and designed into equipment form by IBM, is intended for the encryption and decryption of digital data primarily in commercial applications. It was developed in order to protect from interception or unwanted modification the increasing amounts of information communicated among interconnected computers. The controversy around this standard evolved from a criticism that DES was carefully selected so as to be sufficiently difficult to prevent commercial interception, but not so difficult as to prevent governmental interception by the National Security Agency. Regardless of the ultimate validity of this criticism, the surrounding publicity was the first significant signal of an emerging conflict between civilian and governmental desires for the protection of data.

2.2 Public Key Cryptosystems and the RSA Algorithm

Shortly after the emergence of the DES criticism, a scientific discovery at Stanford and MIT further increased the civilian/governmental cryptology tension and introduced university research as an important new ingredient of the emerging controversy. This discovery consisted of encryption/decryption schemes developed by Diffie and Hellman of Stanford, called Public Key Cryptosystems, and specific encryption/decryption functions for the schemes, developed by Rivest, Shamir and Adleman of MIT, called the RSA Algorithm. The combined discovery received a good deal of attention from the popular press and was characterized as putting an end to traditional cryptology. This discovery is important because it allows construction of a code which can be broken only by finding the solution of an extremely complex and time consuming mathematical problem, thereby suggesting that the code is, in effect, unbreakable. Moreover, this approach makes possible not only the protection of data being communicated, but also the authentication of such data as indeed originating from a legitimate source rather than from an impostor.

The MIT Laboratory for Computer Science (LCS) was in the process of sending out copies of its Technical Memorandum #82 describing the RSA Algorithm, when a new development took place—a letter was written in September 1977 by J.A. Meyer, an NSA employee, who said that he was acting in his own behalf. The letter was addressed to the Information Theory Group of the Institute of Electrical and Electronic Engineers (IEEE). It warned the IEEE scientists (Hellman and Rivest included) who were planning a cryptology symposium for October 1977, that, by holding this symposium and publicly communicating their research results, they might be violating the Department of State's International Traffic in Arms Regulations (ITAR). As explained in Section 4.1 of this report, ITAR controls the flow of military hardware and certain technical data on military technology to foreign countries. According to the Meyer letter, dissemination of such results before a group of foreign scientists who were planning to attend the symposium, or by reports sent to the Soviet Union, could be regarded as export of technical data controlled by ITAR, and hence as a violation of those regulations.

The cryptology symposium discussed above did take place, after some changes were made in the presentations to limit discussion to mathematical issues. At MIT/LCS, as a result of the Meyer letter, we stopped dissemination of Technical Memorandum #82, pending determination of the legality of its publication by our attorneys. We and out that

there was no clear legal answer to this question. In particular, the laws and regulations surrounding ITAR appeared to be overly complex and bewildering. Strict interpretation of their language would yield the absurd conclusion that these regulations had been violated by industry and academia for many years. Yet there were hardly any legal precedents governing such violations and our lawyers felt that strict enforcement of the applicable regulations would most likely be viewed by the courts as unconstitutional. This opinion was to be later reinforced by a memorandum prepared by the U.S. Department of Justice for the Science Advisor to the President.

To understand better the government's views on these regulations, and to alert the Government to our views on the future importance of public cryptology (see Section 5.1), we initiated two meetings. One, at MIT, was with the President's Science Advisor, Dr. Prange; the Deputy Undersecretary of Defense in charge of Intelligence, Dr. Dineen; the Deputy Director of the NSA, Mr. Rosenblum; and the Director of MIT/LCS, Prof. Dertouzos. The other meeting was a visit of Professor Rivest and Dertouzos with Mr. Rosenblum at the NSA. These meetings, five years ago, reinforced our views on the markiness of ITAR and left us with a feeling that the Government did not fully share our concerns on the future evolution of the information field. Nevertheless, there was a willingness on both sides to try to find a workable scheme that would protect our mutual interests. To that end, MIT proposed at one of these meetings an approach that was later to become part of our recommended MIT policy in cryptology. Under this approach, the MIT/LCS, as the locus of cryptology research at MIT, volunteered to send all cryptology papers to the NSA at the same time that they are sent to the author's close colleagues for technical comment in proposing this We made clear our intent that these papers would be sent to the NS for their information and not for securing their permission to publish.

Shortly after these meetings, in the absence of any clear answer to our questions on legality, and in view of our volunteered action, we informed the DOD that we were resuming publication of LCS Technical Memorandum #82.

2.3 The Davida Secrecy Order

In early 1978 George I. Davida, Professor of Computer Science at the University of Wisconsin-Milwaukee, applied for a patent on a novel cryptographic scheme. In April 1978 he received a letter from the Department of Commerce which ordered him not to discuss or write about the principles in this cryptographic scheme. This invocation of a patent secrecy order by Commerce under the Invention Secrecy Act raised considerable objections in the academic community, notably from Wisconsin's Chancellor Werner Basse who, according to Science (July 14, 1978), was outraged at what he regarded as an invasion of his faculty's academic freedom without due process.

The secrecy order was lifted shortly thereafter and, as in prior incidents, the main crisis was averted while the surrounding discussion served to increase awareness and concerns about the possibility of more serious conflicts between the university and government.

2.4 The ACE Public Cryptography Study Group

In March 1980, in response to a request by the NSA, the American Council on Education (ACE)—a group of university administrators—established a Public Cryptography Study Group. The NSA's concern that led to formation of this group was expressed by Vice Admiral Bobby Inman, Director of the Agency, who felt that information contained in published articles and monographs on cryptology endangered the national security.

The group, after meeting for a year, recommended a voluntary prior restraint procedure under the following guidelines:

1. NSA would notify the cryptologic community, including authors and publishers, of its desire to review manuscripts concerning aspects of cryptology prior to publication.
2. NSA, in consultation with appropriate technical societies, would define as precisely as possible those aspects of cryptology to be covered by the procedure.
3. NSA would invite authors to send manuscripts to NSA for review prior to publication.
4. NSA would assure prompt review by its staff of submitted manuscripts and prompt response to authors with an explanation, to the extent feasible, of proposed changes, deletions, or delays in publication, if any.
5. NSA would provide, in the case of unresolved disagreements, the opportunity for authors to obtain prompt review by an Advisory Committee of five persons (two appointed by the Director of NSA and three appointed by the Science Advisor to the President from a list of nominees provided by the President of the National Academy of Science), which would make a recommendation to the Director of NSA and to the author concerning the matters in issue. Members of the Advisory Committee shall have adequate clearance so that the committee can make informed recommendations.
6. There would be a clear understanding that submission to the process is voluntary and neither authors nor publishers will be required to comply with suggestions or restrictions urged by NSA.

At MIT, we reacted negatively to some of these recommendations and declared our preference for our own approach for the following reasons:

1. Under the ACE scheme, researchers carry the burden of deciding what papers to submit to the NSA for review. Under the MIT scheme, all papers in cryptology are submitted, thereby relieving the researcher from decisions that necessarily must be based on partial knowledge as to what may or may not require classification.
2. A researcher who adheres to the ACE scheme accepts restraints prior to the publication of research results. The MIT scheme does not involve prior restraint.
3. Even though it is voluntary, the ACE scheme may be viewed as practically obligating researchers to comply. Moreover, several researchers felt that the voluntary aspect of the ACE scheme was a test and a first step toward eventual formalization of prior restraint as a non-voluntary basis.

2.5 The NSF Policy Changes

In August 1980, the National Science Foundation (NSF), at NSA's prodding, told MIT computer scientist Leonard Adleman (then on leave at the University of Southern California), that part of his NSF cryptology research grant proposal would not be funded. We believe that this was the first instance in NSF's grant history that funds were refused for reasons of national security. At the same time, Professor Rivest of MIT was also notified by the NSF that his pending proposal would probably meet with the same fate.

Subsequently, Adleman received a call from Admiral Inman who indicated that the NSA wanted to fund his proposal. The offer was refused by Adleman who was concerned about accepting funds from the NSA when he had applied to the NSF. Eventually, NSF granted Adleman the entire sum that he had requested, but included language in the grant letter that in effect made Adleman responsible for applying prior restraint.

The NSF diffusion in cryptology research resurfaced later in mid-1981 in

connection with the Rivest proposal. Prior to that time, the NSF had established a subcommittee, under the leadership of Professor John Guting of MIT, to recommend NSF policy changes for dealing with cryptology research. The Guting report recommended a scheme similar to that adopted by MIT for informing the NSA of relevant research results. Subsequently, the NSF notified MIT of changes in its grant policy which, in opposition to its own subcommittee recommendations, required a prepublication review. The new language in Section 704C of the NSF Grant Policy Manual was as follows: "When in the course of an NSF supported project information or materials are developed which may affect the defense and security of the United States, the grantor: (i) has the responsibility to notify immediately the cognizant NSF Program Director of any data, information or materials developed under an NSF-supported project which may require classification; (ii) shall prior to dissemination, distribution or publication of the potentially classifiable research results allow NSF the option of reviewing such materials; (iii) shall, upon receipt of notice from the cognizant NSF Program Director of NSF's intention to exercise its option, defer dissemination, distribution, or publication pending exercise by NSF of its option of review and determination that the results are not classified, and when requested by the NSF Program Director, direct the potentially classifiable materials to the NSF Security Officer, 2800 G St., N.W., Washington, D.C. 20560. Provided further, however, that such deferral is subject to NSF's review and determination being completed within 60 days of receipt by NSF of such material."

We objected to this language primarily because it imposed prior restraint on potentially classifiable research results—a serious phrase which would apply not only to cryptology but to all NSF supported research.

The language that was finally negotiated between NSF and MIT for the Rivest grant was based on the exact language of Presidential Executive Order 12065, (the precursor of the Executive Order discussed in Section 4.4) and was as follows:

In these rare instances when data, information, or materials developed in the course of a project supported by NSF are believed to require classification, the grantor: (i) has the responsibility to notify immediately the cognizant NSF Program Director; (ii) shall, prior to dissemination, distribution, or publication of such data, information, or materials allow NSF the option of reviewing them; (iii) shall, upon receipt of notice from the cognizant NSF Program Director of NSF's intention to exercise its option, defer dissemination, distribution, or publication pending exercise by NSF of its option of review and determination by the appropriate agency that the materials are not classifiable and when requested by the NSF Program Director, direct the potentially classifiable materials to the NSF Security Officer, 2800 G Street, N.W., Washington, D.C. 20560. Provided further, however, that such deferral is subject to review and determination being completed within sixty (60) days of receipt by NSF of such material.

We agreed to this language because it was essentially identical to the language of the Executive Order on classification and because of the extreme improbability that it would be invoked.

We subsequently asked the NSF to clarify whether the revised language would apply to all NSF grants as we had understood during our negotiations, or only to the Rivest grant. The NSF has not, as of this writing, responded to our request, leaving ambiguous the degree of applicability of the 60 day time constraint.

3.6 Very Large Scale Integrated (VLSI) Circuit Research

Two factors seem to be at the root of the most development. The first is the progressively increasing involvement of U.S. universities in VLSI research, primarily because of the maturation of the associated design and process technologies. The second involves the Department of Defense's desire in 1980 to establish a research and development program for very high speed integrated circuits (VHSIC—pronounced vee-sick)—a subclass of very fast VLSI circuits capable of working in thermally and radioactively hot environments for use in the control and instrumentation of weapons. These factors led to questions about the participation of foreign students and faculty in VLSI research and the export of technical data concerning weapons technology. In addition to the ITAR-based concerns, these developments brought into focus the Department of Commerce's Export Administration Regulations (EAR). The EAR, discussed in Section 4.3, are intended to control the export of critical technologies with dual military and civilian uses. Finally, it seems that several people within government began to be progressively more concerned with the economic advantage afforded foreign nations, notably Japan, through easy export of our forefront technologies.

These governmental concerns, which were reflected in discussions with universities about contractual arrangements for VLSI research, along with incidents involving restrictions of foreign scientists at Cornell and MIT, led to substantial and negative academic reactions. The culmination of these academic concerns was a letter signed by the five presidents of California Institute of Technology, Cornell, MIT, Stanford, and the University of California, which was sent in February 1981 to the Secretary of Commerce, Defense, and State (Appendix B). This letter made the case that the contemplated restrictive measure would harm one of the principal technological assets of this nation—university research. The five presidents did eventually receive replies from all three secretaries who tried to reassure the academic community that such controls would not be carelessly invoked. Nevertheless, the academic community remained and still remains unsure of what constraints, if any, would be imposed by the Government on the conduct of such research.

Concerns about academic research were once again raised in January 1982 by Deputy Secretary of Defense, Frank Carucci; Deputy Director of the CIA, Bobby Inman; and Secretary of Defense, Casper Weinberger. Carucci set forth in *Science* (January 8, 1982) examples of Soviet scientists who, after working in U.S. universities, return to weapons development in the USSR, and of USSR exploitations of senior-scholar exchanges, whereby Soviet scientists interested in military applications of research are prepared, while we prepare scholars interested in the humanitarian issues, speaking before the American Association for the Advancement of Science (AAAS) meeting of January 7, 1982, called for prepublication review of university research results in cryptography, computer hardware and software, laser, crop projections and manufacturing processes. Weinberger stated that the Service "have organized a massive, systematic effort to get advanced technology from the West."

As of the writing of this report, there has been no resolution of these most recent issues involving the prepublication review of results, and the participation of foreign scholars in critical university research areas.

3.7 The Report of the Defense Science Board Task Force

In January 1982 the "Report of the Defense Science Board Task Force on University Responsibilities to National Security Requirements" was submitted to the Secretary of Defense through the Office of the Under Secretary of Defense for Research and Engineering. This report was prepared in response to a House Armed Services Committee request and addressed several issues associated with DOD sponsorship of university research.

With respect to export control, the flavor of the report is captured by the following two excerpts:

DOD is caught in a dilemma. If it vigorously attempts to regulate the flow of scientific information in the scientific community, it could jeopardize the strength and vitality of the very community it is seeking to revitalize for the sake of national defense. On the other hand, if DOD abandons any attempt at regulation in the university context, it could seriously compromise and, in certain cases, totally undercut other efforts to control the outflow of military critical technology. The "middle ground" is a difficult one to establish. This Task Force has attempted, if not to solve the problem, to at least lay a framework for solving the issue by means both practicable and, it is hoped, acceptable to the academic community. A dialogue with the universities has already begun over the transfer of non-classified but nonetheless sensitive information in the Very High Speed Integrated Circuits (VHSIC) Program.

The focal point for control is the DOD contract: the Government negotiates the terms of the release of information with the contractor. The Project Office or Contract Monitor within DOD thus becomes the interpreter of military criticality and the extent to which ITAR or EAR is applicable. The system is voluntary in the sense that the contract does not have to be accepted. If guidelines for release of information are accepted as part of the contract, then there should be little room for misunderstanding later. It could be argued that restrictions such as these violate the spirit of academic freedom and will curtail the free flow of information required for maintaining a healthy dialogue within the scientific community. This might be true if DOD were seeking to restrict the flow of all scientific information directly or indirectly related to military capability. This, however, is clearly not the case. The Department of Defense is assiduously rejecting any control guidelines that would restrain the development and dissemination of the fruits of basic research.

This report may have been the first to emphasize the use of the research contract as the instrument of control, rather than placing reliance upon more generalized devices such as ITAR or EAR.

3.8 The Corson Report

In September 1982, an important report entitled "Scientific Communication and National Security" was issued by the Panel on Scientific Communication and National Security of the Committee on Science, Engineering and Public Policy of the National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine. This document, known as the Corson Report after the Panel's Chairman Dale R. Corson, sets forth a set of principles aimed at resolving the complex issue that is the subject of our report, i.e., the conflict between the national objectives of economic competitiveness and national security.

The Corson Report discusses: (1) the essential transfer of military significant U.S. technology to the Soviet Union; (2) the importance of operations for the principal mission of U.S.

universities; (3) the current control system; and (4) the costs and benefits of these controls. The key recommendations of the Corson Report are:

1. On the control of university research activities, the panel identifies three categories of research—clearly open, clearly classified and a small "gray area" for which limited restrictions short of classification are appropriate. In the language of the Corson Report:

The Panel recommends that no restriction of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involves a technology meeting all the following criteria:

- *The technology is developing rapidly, and the time from basic science to application is short;*
- *The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;*
- *Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and*
- *The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.*

The panel recommends that in the limited number of instances in which all of the above four criteria are met but classification is unwarranted, the values of open science can be preserved and the needs of government can be met by written agreements no more restrictive than the following:

- a) *Prohibition of direct participation in government-supported research projects by nationals of designated foreign countries with no attempt made to limit physical access to university space or facilities or enrollment in any classroom course of study. Where such prohibition has been imposed by visa or contractually agreed upon, it is not inappropriate for government-university contracts to permit the government to ask a university to report those instances coming to the university's attention in which the stipulated foreign nationals seek participation in any such activities, however supported. It is recognized that some universities will regard such reporting requests as objectionable. Such requests, however, should not require surveillance or monitoring of foreign nationals by the universities.*
- b) *Submission of stipulated manuscripts simultaneously to the publisher and to the federal agency contract officer, with the federal agency then having 60 days to seek modifications in the manuscript. The review period is not intended to give the government the power to order changes. The right and freedom to publish remain with the university, as they do with all unclassified research. This does not, of course, detract from the government's ultimate power to classify in accordance with law any research it has supported.*

The panel recommends that in cases where the government places such restrictions on scientific communication through restrictive or other written agreements, it should be obligated to record and tabulate the instances of these restrictions on a regular basis. The provisions of EAR and ITAR should not be invoked to deal with gray areas in government-funded university research.

2. On the export of domestically available technical data under EAR and ITAR:

1. *The Panel recommends that unclassified information that is available domestically should*

receive a general license exemption from the formal licensing process.

2. *The Panel recommends that information that is not directly or significantly connected with technology critical to national security should also receive a general license exemption from the formal licensing process. The critical technology list approach—if carefully formulated—could serve to define those limited areas in which controls are appropriate.*

3. On the use of voluntary controls: *The Panel concludes that the voluntary publication control mechanism developed for cryptography is unlikely to be applicable to other research areas that bear on national security. However, the Panel recommends that consideration be given to adopting this mechanism in future cases, if and where the appropriate preconditions exist.*

4. On the Militarily Critical Technologies List (MCTL): *The Panel recommends a drastic streamlining of the MCTL by reducing its overall size to concentrate on technologies that are truly critical to national security.*

5. Finally, on technology transfer to the third world, the panel reached no conclusions and recommended further study.

In the above summary we have emphasized, through inclusion of more extensive quotations, the Corson Report recommendation on the control of university research activities because we comment on it further in Section 4.3 of this report.

4. THE LEGAL FRAMEWORK

4.1 Introduction

The control of technological information by the U.S. Government falls under one of the following principal categories of laws and regulations:

1. The Arms Control and Export Act of 1976 (ITAR)
2. The Export Administration Act of 1979 (EAR)
3. The Executive Order on National Security Information.

These are discussed in more detail in the three subsections that follow.

In addition, there is: (1) the Atomic Energy Act of 1954 which established the "born secret" concept, i.e., the notion that new results or even unclassified material presented in a new way can be called classified; (2) the Invention Secrecy Act (ISA) which permits the classification of patents involving national security; (3) the Freedom of Information Act which contains provisions for exempting agencies from having to disclose certain types of information; (4) the Executive Order on Intelligence (December 1961) which allows for the covert collection of information by agents posing as journalists or academicians; and (5) various scientific and cultural exchanges with respect to which the Department of State places restrictions on foreign visitors. These five vehicles are tangential to our concerns and will not be discussed further. They may, however, assume renewed importance as new developments emerge.

Finally, there are two potentially significant ways in which the Government could exercise control over the export of technological information—the research contract and the Immigration and Nationality Act which we discuss in Section 4.3.

4.2 The Arms Control and Export Act of 1976 (ITAR)

The International Traffic in Arms Regulations (ITAR) has been born under the Department of State in fulfillment of the Arms Control and Export Act.

Under the ITAR, all non-exempt equipment listed in the United States Munitions List as "items, or technical data and information of war," as well as

related classified and unclassified technical data, may not be exported except under a license issued by the Office of Munitions Control of the State Department. The ITAR definition of "export" is broad, particularly with respect to the export of technical data:

The export controls of this subchapter shall apply whenever the information is to be exported by oral, visual or documentary means. Therefore, an export occurs whenever technical data is, *inter alia*, mailed or shipped outside the United States, carried by hand outside the United States, disclosed through visits abroad by American citizens (including participation in briefings and symposia) and disclosed to foreign nationals in the United States (including participation in briefings and symposia).

The Office of Munitions Control, in Munitions Control Newsletter No. 80 (February 1980), has further clarified and limited the ITAR's licensing provisions as applied to unclassified cryptologic technical data. As that newsletter states:

Cryptologic technical data for which a license is required under Section 121.01, Category XVIII, is interpreted by this office with respect to information relating to Munitions List items in Categories XI (c) and XIII (b) to include only such information as is designed or intended to be used, or which reasonably could be expected to be given direct application, in the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of items in such categories. This interpretation includes, in addition to engineering and design data, information designed or reasonably expected to be used to make such equipment more effective, such as encoding, or enciphering techniques and systems, and communications or signal security techniques and guidelines, as well as other cryptographic and cryptanalytic methods and procedures. It does not include general mathematical, engineering or statistical information, not purporting to have or reasonably expected to be given direct application to equipment in such categories. It does not include basic theoretical research data. It does, however, include algorithms and other procedures purporting to have advanced cryptologic application.

The United States Court of Appeals for the Ninth Circuit has limited substantially the scope of the ITAR. According to that Court, the ITAR "prohibits only the exportation of technical data significantly and directly related to specific articles on the Munitions List" and, in circumstances where the data could have both military and peaceful applications, such prohibitions is enforceable only to the extent that the exporter knows—or has reason to know—that the information is intended for the prohibited (military) use. (*United States v. Edler Industries, Inc.*)

Unauthorized export of materials or data included on the Munitions List—if "willful"—can result in fines of up to \$100,000 and/or imprisonment for up to two years. The Act provides for civil penalties as well.

The ITAR must be viewed as an imperfect tool for restricting the transfer of "technical data." Its infirmities may well explain the NSA efforts to construct, through dialogue, the informal mechanisms recommended by the ACE Committee. The problems of ITAR are as follows:

First, no one really knows what the definition of "technical data" encompasses and how it might specifically apply to cryptological information. The difficulty of clarifying this definition is exemplified by the Department of State's interpretive circulars ("Memorandum No. 88" which asserts that "technical data" does not include mathematical concepts, but includes certain algorithms—a technically ineffective position since the word "data" means information

algorithm is often a straightforward process.

Second, the ITAR has no application to information in the public domain. Thus, publication in *Science* or *Scientific American* not only disseminates the information, it effectively removes ITAR's application to the published information.

Third, as already discussed, the leading legal precedent, *U.S. vs. Edler Industries*, reads into ITAR's scienter requirement, meaning that the person disclosing the information to a foreign national must do so with knowledge or reason to know that the foreign national intends to use the information in a prohibited and use—an intention probably absent and difficult to prove in the academic environment.

Finally, the Department of Justice itself has raised serious concerns about the constitutionality of ITAR on the grounds that it operates as a prior restraint on free speech without the usual safeguards of judicial review.

4.3 The Export Administration Act of 1979 (EAR)

In an attempt to clarify uncertainties in United States export control policies and to stifle such policies in furtherance of national security, foreign policy and economic objectives, Congress enacted the Export Administration Act of 1979, replacing the Export Administration Act of 1949.

Acting under this authority, the Department of Commerce has issued a lengthy series of Export Administration Regulations (EAR). Exports subject to licensing under the EAR—including specified commodities and related technical data—require approval from the Office of Export Administration, Department of Commerce, in the form of a license.

The defense articles and defense services on the U.S. Munitions List are expressly excluded from the EAR licensing framework. Nevertheless, included among the list of commodities for which a validated export license is required are:

Cryptographic equipment and ancillary equipment (such as teleprinters, perforators, vocoders, visual display units) designed to ensure secrecy of communications (such as telephony, telephony, facsimile, video, datalog or stored information, their specialized components, and software controlling or performing the function of such cryptographic equipment. Also video systems which, for secrecy purposes, use digital techniques (conversion of an analog, i.e., video or facsimile, signal into a digital signal). (This item also covers digital computers and differential analyzers (numerical computers) designed or modified for, or combined with, any cipher machines, cryptographic equipment, devices or techniques including software, microprogram (hardware), and equipment or systems incorporating such computers or analyzers, except simple cryptographic devices or equipment only ensuring the privacy of communications.

Assuming that certain cryptographic equipment falls outside of Department of State jurisdiction but within the purview of the EAR, the Commodity Control List indicates that such equipment may not be exported to any nation except Canada without a license. Further, the list indicates that the reason for control of such equipment is national security. This being the case, the Secretary of Defense is authorized to review any proposed export of such equipment or related technology for the purpose of determining whether such export would "make any contribution, which would prove detrimental to the national security of the United States, to the military potential of such (foreign) country or any other country."

Technical data is treated as distinct from commodities under the EAR, and is regulated in depth. The relevant section defines technical data as follows:

of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a tangible form, such as a model, prototype, blueprint, or an operating manual; or they may take an intangible form such as technical services.

The definition of what constitutes an "export" of such data is as broad as that contained in the ITAR. Three categories are identified:

(1) "Export of Technical Data" means

(i) An actual shipment or transmission of technical data out of the United States; (ii) Any release of technical data in the United States with the knowledge or intent that the data will be shipped or transmitted from the United States to a foreign country; or (iii) Any release of technical data of U.S. origin in a foreign country.

(2) Reexport of technical data. "Reexport of technical data" means an actual shipment or transmission from one foreign country to another, or any release of technical data of U.S. origin in a foreign country with the knowledge or intent that the data will be shipped or transmitted to another foreign country. Technical data may be released for reexport through:

(1) visual inspection of U.S.-origin equipment and facilities abroad; (2) oral exchanges of information abroad; and (3) the application to situations abroad of personal knowledge or technical experience acquired in the United States.

There is a so-called "General License"—that is, a license granted automatically by EAR without the need of application—for technical data falling in the following categories:

(a) Data generally available. Data that have been made generally available to the public in any form, including: (1) Data released orally or visually at open conferences, lectures, trade shows, or other media open to the public; and (2) publications that may be purchased without restrictions at a nominal cost or obtained without cost or are readily available at libraries open to the public. The term "nominal cost" as used in paragraph (2) of this section is intended to reflect realistically only the cost of preparing and distributing the publication and not the intrinsic value of the technical data. If the cost is such as to prevent the technical data from being generally available to the public, General License GTDA would not be applicable.

(b) Scientific or educational data. (1) Dissemination of information not directly and significantly related to design, production, or utilization in industrial processes, including such dissemination by correspondence, attendance at, or participation in, meetings; or (2) instruction in academic institutions and academic laboratories, excluding information that involves research under contract related directly and significantly to design, production, or utilization in industrial processes.

(c) Patent applications. Data contained in a patent application prepared wholly from foreign origin technical data where such application is being sent to the foreign inventor to be secured and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office. (No validated export license from the Office of Export Administration is required for data contained in a patent application, or an amendment, modification, supplement or division thereof for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office in 37 CFR Part 2. See § 279.106.)

Willful violations of the EAR licensing provisions can result in fines up to \$50,000 and imprisonment for up to five years. There is no reported case law interpreting the technical data provision of the EAR.

A working group is currently drafting a new list of Military Critical Technology which is expected to be rather broad in its coverage, and a new set of regulations has been drafted but has been stalled at least for the time being, because of legislative reactions by the scientific community.

4.4 Executive Order 12386 on National Security Information

On April 2, 1980, President Reagan signed Executive Order No. 12386 replacing Executive Order No. 12065 which had been promulgated by the Carter Administration. The new Order reverses many of the presumptions of the prior Order and in general makes classification easier. In its draft form, the new Order had eliminated the exception according to which "basic scientific research information not clearly related to the national security may not be classified." This exception was eventually reinstated and now appears in the current Executive Order following vigorous opposition to its elimination by the academic community, led by MIT President Paul E. Gray.

The complete scope of the new Executive Order is not clear. By its terms, it extends to all information that is "owned by, produced by or for, or is under the control of the United States Government". Informal interpretations include all work sponsored by the federal government. (There is some concern that the new Order's elimination of an exception for private sector research can be read as a signal that the new Order extends to private sector research, but any such intention has been informally denied by the Administration.)

The most important new provision affecting universities is Section 1.305 which provides:

1.305. Exceptional Cases. When an employee, contractor, licensee, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this Order and its implementing directives. The information shall be transmitted promptly as provided under this Order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within thirty (30) days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for classification determination.

The obligation placed upon a contractor or grantee originating information to forward that information under this section is uncertain since it requires formation of a "belief" that the information requires classification. (See also Section 3.3 for the MIT-NSA agreement which involves this requirement.) Another portion of the Order (1.10c) addresses the problem with the provision "If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified pending a determination by an original classification authority." It would be open to the Government to contend that safeguarding is required if the grantee has reasonable doubt about the need to classify.

If information is classified, it may not, under penalty of criminal sanctions, be disclosed to anyone without government

tal clearance. The restriction is absolute.

Finally, unlike the ITAR which restricts "export of information to foreign nationals", classification restrictive disclosure of information to anyone.

4.5 Contract Terms and the Immigration and Nationality Act

In addition to the above laws, there is evidence that the Government is considering the use of contract and grant terms in federally sponsored research as a means of controlling the dissemination of research results. Such restrictions entered into voluntarily by grant recipients and contractors may avoid the constitutional doubts surrounding ITAR and EAR and may become the most effective means for controlling the flow of scientific information. The Defense Science Board Task Force on University Responsiveness has suggested (see Section 3.7), and the Department of Defense is reportedly considering, a mechanism which would focus control of research results on the negotiation process at the time of the government grant or contract.

Another potential controlling mechanism may evolve from the Immigration and Nationality Act which empowers the Government to refuse admission to an alien if there is reason to believe that the alien will "engage in activities which would...endanger the welfare, safety, or security of the United States." In addition, an alien may be deported for failing to comply with the conditions under which he was admitted. To date, the immigration laws have not been used in any general way to control technology transfer. Recently, however, the Department of State has made formal inquiries to universities of certain foreign areas of research of certain foreign nationals from Communist countries.

4.6 Interpretation and Conclusions

As is evident from the above summaries of the relevant laws and regulations, the legal structure surrounding the control of scientific and technological information is bewildering. Nevertheless, we shall attempt to draw several conclusions.

The regulations appear to be impractical instruments not intended to regulate scientific exchange in the academic world, for the following reasons:

1. At least ITAR and EAR exclude basic research from their sphere of control.
2. The scientist requirement of the Edgar case—that the person disclosing information know that the recipient of the information intends to use it for a prohibited purpose in a foreign country—provides a legal precedent for a similar requirement for EAR.
3. Neither EAR nor ITAR can control information which has already reached the public domain. Thus the Government would find it difficult to prosecute a case where the information disclosed in a meeting had already appeared in some generally available publication.
4. Serious questions have been raised by the Department of Justice about the constitutionality of both the ITAR and the EAR in their present form.
5. It is believed that, to date, no university has applied for a license under the EAR.

Ultimately, we cannot conclude that we should be at ease about the implications of these regulations. On the contrary, the above assessment of a critical proceeding by State or Commerce would create confusion and doubt and could have a chilling effect on our researchers. Moreover it would take the courts several years to make rulings on any of these issues.

Accordingly, we believe that our best approach is to maintain an ongoing

dialogue with the Government for a bilateral exposition of views, issues and concerns; and to initiate a range of MIT policies that address these problems in responsible and effective ways.

5. ISSUES

5.1 Critical Technologies

For the purposes of this report we may regard university research activities as points within a cube, whose dimensions are: (1) basic to applied; (2) civilian to military; and (3) internationally non-competitive to competitive. At one extreme, basic research of only civilian interest with no potential for international competition presents no conflict and can be freely pursued at the university. Equally clearly, research at the opposite extreme does not belong in a university and most probably should be classified. The concerns addressed by this report involve research on so-called critical or sensitive technologies located somewhere in the middle of this cube, i.e., having basic and applied components, dual military-civilian uses, and international competitive interest. This is indeed the case with both cryptography and VLSI research.

Starting with cryptography, we foresee that during the next decade there will be a progressively increasing number of interconnected computers communicating both within and across organizational boundaries. Conceivably, if personal computers continue to grow at their current rate of some one million new units/year the aggregate of geographically distributed systems will extend to individual homes and small businesses as well. In such a future setting we believe that the protection and authentication of data is a mandatory requirement. Recall that by protection we mean that data may be communicated without interception, whereas by authentication we mean the existence of credible means for certifying the signatory of an electronic message.

Data must be protected precisely because the power of computers makes possible the malicious use of these machines in breaking the defenses of a remote installation, selecting data of interest, copying it, and finally erasing all traces of such an invasion. As the use of geographically distributed interconnected systems grows beyond today's banking and business applications to broader financial, legal, medical and governmental services the potential and penalty for such misuse becomes greater. It is for this reason that we assert a societal need for vigorous research in public cryptography. For it is only through cryptographic techniques that the protection and authentication of data can be effectively insured.

In addition, the unconstrained pursuit of cryptographic research is expected to have beneficial intellectual repercussions in allied fields of computer science. More importantly the timing of expected developments strongly suggests that now is the time to pursue effectively such research and thus to gain on the frontiers of theoretical computer science knowledge. The above motivations are unfortunately in conflict with the possible damage that new publicly available cryptographic results can cause in governmental communications and in the acquisition of foreign intelligence.

Proceeding to our second major area, we believe that VLSI research is instrumental to the future evolution of the electrical engineering and computer science disciplines. More specifically, progress in the formation of new systems depends critically on the structure and function of their subordinate components—which are VLSI circuits. Thus, for example, the development of successful speech-comprehension systems appears to depend critically on the design of proper VLSI structures that will be used in large numbers to carry out simultaneously and in parallel many similar information processing operations.

If a viable the speech comprehension is

achieved, it will have, besides the obvious civilian and military applications, international competitive repercussions. Japan, for example, has already embarked on a ten-year project to achieve this goal (the Fifth Generation Computer Project) with the express intent of eventually dominating the world's computer markets. As before, we see here the presence of a commercial conflict, which becomes particularly important in VLSI, because circuits can be easily copied and replicated.

The same argument is applicable to VLSI design techniques, an area where U.S. dominance is expected. In this area, we are concerned with computer-based techniques for effectively designing very small VLSI circuits (e.g., five mm. on each side) containing over 100,000 circuits—a design process that cannot be carried out manually because of inherent complexity. A successful system capable of such design complexity, along with its software components, can be easily copied, perhaps by foreign scholars who participate in this research.

The conflicts of purpose characterized by these examples are further compounded by a confusion of boundaries: In both cryptologic and VLSI research the boundary between what is basic research of civilian interest and what can be used for military or international competitive purposes is very diffuse. Consider, for example the RSA encryption scheme discussed in Section 3.2. That scheme can be viewed as: (1) a mathematical theory that defines certain functions; (2) an algorithm that implements these functions using subordinate functions like multiplication; and (3) one or two VLSI circuits that implement in hardware that algorithm. Here, the creative and most difficult part has been the discovery of the theory—a basic research activity. The conversion of this theory to an algorithm and the subsequent conversion of that algorithm to VLSI circuits are relatively straightforward development activities that can be effectively carried out by any good team of domestic or foreign engineers. Can this research activity be clearly partitioned into non-critical and critical parts?

In conclusion, certain new research activities are by their very nature multifaceted, i.e., they have basic and applied components, and are significant in the international commercial and military areas. The pursuit of such research is essential for the fundamental growth and leadership of U.S. technology, yet the easy "export" of this research is believed undesirable for it may tend to weaken the nation in military and commercial terms.

5.2 The Problems of Technology Export

The export of technology that is the focus of governmental concerns involves the leakage of university research either (1) in the form of research results; or (2) through the training of foreign scholars in critical technologies on U.S. campuses. In cryptography, the NSA is charged with the responsibility of (1) insuring the security of governmental communications; and (2) gathering intelligence from foreign communications. These two parasitic have the technically conflicting objectives of desiring good cryptography for the U.S. and bad cryptography for other countries. Thus, public cryptology work, if successful, usually helps one of these objectives while hindering the other, depending on whether it enables better code-making or better code-breaking.

The financial costs to our Government of the disclosure of critical code-breaking techniques can be measured in billions of dollars. For example, the NSA states that decryption devices for use in our governmental communications must operate securely for several decades to insure: (1) verification of the encryption scheme; (2) operation in the field; and (3) immunity for some time beyond their removal from the field. Moreover, the political costs of losing the security of our own communications, or our ability to rebut foreign intelligence, could be

staggering and probably not subject to financial measure. The NSA, in view of these national security implications, feels that university research on public cryptology should be controlled through publication review.

In the case of VLSI, the governmental concerns center on the leakage of this critical technology through foreign scholars, as well as through the unconstrained publication of research results. Since approximately one third of the engineering graduate students of our major universities are not U.S. citizens, the fears appear to rest on a sound numerical basis. Since VLSI circuits are used in a large variety of applications, including the control and instrumentation of weapons, the Government fears that we are weakening through such a leakage of technology the military strength of the U.S.

In addition, the easy export of forefront VLSI research gives an unfair commercial advantage to the international competition. In brief terms, the Government asks why we freely export precious technology, while paying dearly for foreign imports such as oil and cars.

5.3 The Problems of Constrained Research

The imposition of constraints on research invariably results in a loss of effectiveness. Progress is slower and fewer people, hence fewer good people, are attracted to pursue such research. In addition, certain future opportunities are foreclosed and results that would have otherwise been achieved by a wider, intercommunicating community are either never realized or postponed.

The inherent coupling of research and education in our universities means that constraints on the former necessarily lead to constraints on the latter. As a result, in such a constrained environment we cannot train as effectively the scientists and engineers who after moving to industrial and academic settings will generate this nation's future technological progress.

In addition, and from a geo-political viewpoint, the control of U.S. research in certain critical technologies will tend to weaken our allies and is likely to lead third-world and neutral countries away from the U.S. toward possibly adversary countries for the acquisition of needed technology.

The imposition of constraints on foreign scholars who participate in U.S. university research will lead to reduction of the effective research workforce, place a large number of researchers, hence of good researchers, are not U.S. citizens. In addition, such restrictions will reduce the number of foreign scholars who acquire a first-hand knowledge of our systems—a loss for the U.S., whether such scholars stay in this country or return to their own countries. In addition, the exclusion of foreign scholars from certain research activities is impracticable and creates an unpleasant climate. Impracticable because it is difficult for a university which is predicated on the free pursuit of ideas to police who pursue what ideas, and unpleasant because of the evident discrimination associated with such a restriction.

Finally, in today's eras of multinational corporations, it is not at all clear that control of university research or of the access by foreign scholars will be effective in reducing the overall leakage of critical technologies.

Taken together, these consequences suggest that such constraints are likely to reduce our overall technological leadership and weaken the very strengths that they are intended to protect.

6.1 Introduction

The arguments of the preceding section have led us to search for effective means that can allow governmental concerns while preserving the fundamental strength of unconstrained research. There is clearly no perfect solution that can thoroughly satisfy both sides of this conflict. Accordingly, we have approached this serious problem with a degree of flexibility and a tolerance for less than perfect solutions. The balance on which we have settled is embodied in our recommendations for a relevant MIT policy which is presented next along with a summary of our reasons.

6.2 Recommended MIT Policy

We believe that one important part of MIT's mission is to prepare our society for a technologically advanced future. To do this, we must continue to pursue leading-edge research in areas that we believe to be of future significance, and to prepare the future professionals in forefront technologies. Current and expected developments in communication, information systems and other areas of science and technology call for continued intensive research and development efforts on our part. In some areas, e.g., very large scale integrated circuit design (VLSI), continued academic involvement is also central to the evolution of the underlying disciplines. In this case electrical engineering and computer sciences. At the same time, serious concern has been expressed about some technology transfer resulting from normal university activities in these areas. We therefore believe it necessary to state our policy with respect to this issue.

Freedom of inquiry and freedom to communicate are essential features of a university. Accordingly, we must be able to teach and perform research in an atmosphere where ideas are freely pursued and exchanged. MIT's role in advancing technology should continue in this open atmosphere. It is also true we believe, that scientific and technological progress are best secured in an open atmosphere, and that the scientific costs to the nation of imposing restrictions outweigh the benefits. Openness also requires that as a general policy MIT not undertake classified research, or research whose results may not be freely published without prior permission. We believe that openness of the university also requires that, once they are among us, foreign students, faculty and scholars should be on an equal basis with their U.S. counterparts in their access to MIT academic and research projects. Moreover, restrictions on access to ideas or places within a university are difficult to enforce and likely to be ineffective.

Exceptions to these policies regarding publication, classification and foreign students and scholars may be made, but only in those very rare instances where the area of work is crucially important to MIT's educational mission and the exception is demonstrably necessary for the national good. If these conditions are not met, MIT will decline or discontinue the activity and, if appropriate, propose it for consideration off-campus or elsewhere.

MIT, like other universities, has a responsibility to the national interest. When sensitive but unclassified research at MIT is important to the national security we will take appropriate steps to ensure that the relevant government agencies are informed of the results. For example, it is our current policy to inform the U.S. Government of our research in information protection and cryptography by sending publication material in this area to the NSA at the same time that we send it to our class colleagues or technical contacts. As a further example, we have also agreed with the NSP that in those rare

certain of our cryptography research results require classification, we will submit them for review to the cognizant government agency prior to dissemination.

Government officials are urged to recognize the concern that bureaucratic forces are likely to try to convert exceptional circumstances into rules. We urge them to resist such forces.

6.3 Relationship of MIT Policy to the Corson Report

In view of the significance of the Corson Report, (see Section 3.7) and the similarity of the issues and recommendations addressed by both the Corson and MIT reports we make the following comments:

We are in full agreement with the principles of the Corson Report. Our concerns stem from the possible misinterpretation of the Report's specific criteria under which "grey area" research may be subject to restrictions and of its specific methods for implementing such restrictions. In particular, we fear that its detailed recommendations may be interpreted and implemented in ways which ignore their accompanying qualifications. If indeed such qualifications are ignored, the Corson Report recommendations could be read as restrictive imperatives.

Our own policy in Section 6.2 above calls for openness of communication and equality among foreign nationals and their U.S. peers. "Exceptions may be made but only in those very rare instances where the area of work is crucially important to MIT's educational mission and the exception is demonstrably necessary for the national good." By not specifying, a priori, the criteria for or the general nature of such exceptions, we feel that the danger of converting qualified examples into rules is mitigated.

COMMITTEE ON THE CHANGING NATURE OF INFORMATION Membership

Richard B. Adler (since May 1981)
MIT Associate Department Head for Computer Science and Electrical Engineering

Michael L. Dertouzos, (Chairman)
Director, MIT Laboratory for Computer Science

John M. Deutch
Dean, MIT School of Science

George H. Dummer (since May 1981)
Director, MIT Office of Sponsored Programs

Professor Herman N. Eisen (since April 1982)
Professor of Immunology
MIT Department of Biology

Carl B. Feldbaum (through May 1981)
Attorney, Palomar Corporation

Francis E. Low (ex-officio)
MIT Provost

Jeffrey A. Maidman
Senior Lecturer in MIT Sloan School of Management

Student Affairs

Louis Menand, III
MIT Special Assistant to the Provost
Senior Lecturer in MIT Department of Political Science

Robert C. Merwin (through October 1981)
Professor of Management
MIT Sloan School of Management

Ronald L. Rivest
Professor of Computer Science
MIT Department of Electrical Engineering and Computer Science

Walter A. Rosenblith
Institute Professor and Past MIT Provost

Kenneth A. Smith (ex-officio since July 1981)
MIT Associate Provost and
Vice President for Research

Robert E. Sullivan
Partner, Herrick and Smith

Judith J. Thomson
Professor of Philosophy
MIT Department of Linguistics and Philosophy

Gerald L. Wilson (since April 1982)
Dean, MIT School of Engineering

APPENDIX B THE FIVE PRESIDENTS' LETTER

The Five Presidents' Letter

February 27, 1981

The Honorable Malcolm Baldrige
Secretary of Commerce
14th Street
Washington, D.C. 20230

The Honorable Alexander M. Haig, Jr.
Secretary of State
2201 C Street, N.W.
Washington, D.C. 20520

The Honorable Casper Weinberger
Secretary of Defense
The Pentagon
Washington, D.C. 20301

Dear Messrs. Baldrige, Haig, and Weinberger:

We are writing to request clarification of the applicability of certain export restrictions to teaching and research activities conducted by American universities. We are deeply concerned about recent attempts to apply to universities the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Examples of such efforts by government agencies include a December 12, 1980, memorandum by the Director of the Very High Speed Integrated Circuit (VHSIC) Program Office, attempts to restrict publication of unclassified university research results arising from DOD-sponsored projects, and a Department of Commerce mandate to at least one university barring certain foreign scholars from that university's sponsored research activities due to their citizenship. Unfortunately, these initiatives appear to be only the first of many such actions to follow.

The ITAR and EAR regulations have existed for a number of years, and have not until now been applied to traditional university activities. The new construction of these regulations appears to contemplate government restrictions of research publications and of dissemination among scholars, as well as discrimination based on nationality in the employment of faculty and the admission of students and visiting scholars. In the broad scientific and technical areas defined in the regulations, faculty would not conduct classrooms lectures when foreign students were present, engage in the exchange of information with foreign visitors, present papers or participate in discussions at symposia

and conferences where foreign nationals were present, employ foreign nationals to work in their laboratories, or publish research findings in the open literature. Nor could universities, in effect, admit foreign nationals to graduate studies in those areas. Such restrictions would conflict with the fundamental precepts that define the role and operation of this nation's universities.

The regulations could be interpreted to cover instruction and research which, although potentially useful in military applications, have much broader utility in such other areas as medical systems and communication equipment. Such interpretations of the regulations, coupled with their severe criminal penalties, could have a very real and unintended chilling effect of legitimate academic exchange.

Restricting the free flow of information among scientists and engineers would alter fundamentally the system that produced the scientific and technological lead that the government is now trying to protect and leave us with nothing to protect in the very near future. The way to protect that lead is to make sure that the country's best talent is encouraged to work in the relevant areas, not to try to build a wall around past discoveries.

It should be recognized that the only realistic way to "maintain" VHSIC research is to classify the whole program. In our view this would be self-defeating: the entire endeavor, including high technology cannot be put back into the bottle. Furthermore, most universities have concluded that performance of classified research is incompatible with their essential purpose. University committees could prefer, for the most part, to change their field of interest rather than have their research and teaching so constrained. Funding high technology research via universities would decrease our nation's competitive position, since the research would have to be carried out elsewhere and less effectively in a classified atmosphere. Moreover, we would lose the restrictions free of these problems from the university programs which have been contributing up to this point. Elimination of such working and research from academic laboratories would endanger the future of graduate programs in engineering, computer science, and related fields, and would result in a tremendous loss of potential high technology expertise available to American industry. The new restrictions

they fail to protect the status quo and virtually guarantee that there will be no future.

Moreover, application of export restrictions to universities would pose significant practical difficulties. It would be virtually impossible for most universities to administer such restrictions given the necessarily decentralized and fluid nature of most campuses. Because it is so inconsistent with their character, universities are neither structured nor staffed to police the flow of legitimate visitors to a given laboratory or the dissemination of information by their faculty at international conferences, or, indeed, even in a campus classroom where foreign students happen to be present.

The December 12, 1960, memorandum mentioned earlier pertaining to the

can be differentiated from areas such as device design and fabrication techniques, process equipment, and software, for which approval of publication or presentation normally would be denied. Such distinctions are proposed to be made by government employees, using criteria of questionable reliability and suitability.

There is no such easy separation in any engineering curriculum intended to be relevant to our national industrial needs and problems. Furthermore, producing graduates with no "hands-on" experience in these areas would be of little value to American high technology industries.

The proposed extension of the restrictions to university activities ought not be made without a thorough assessment of the policy implications, the necessity and prospective effectiveness of the

the established role and operations of universities, and the serious legal and constitutional questions raised.

In the interim, it might be mutually advantageous for DOD to continue (selectively and sparingly) to rely on its classified research facilities to carry out the most sensitive segments of the VHSIC program. That has been its practice in previous years, and is far preferable to the application of these restrictive and virtually unenforceable regulations to universities. For those university activities which remain unclassified, we urge the government to cease all attempts to apply the restrictions until the broader issues are resolved.

We hope that after examining this issue carefully, you will clarify what has always been our understanding—namely, that the regulations are not

arising from unclassified research and teaching.

Sincerely yours,

Donald Kennedy
President, Stanford University

Marvin L. Goldberger
President, California Institute
of Technology

Paul E. Gray
President, Massachusetts
Institute of Technology

Frank H. T. Rhodes
President, Cornell University

David S. Saxon
President, University of
California

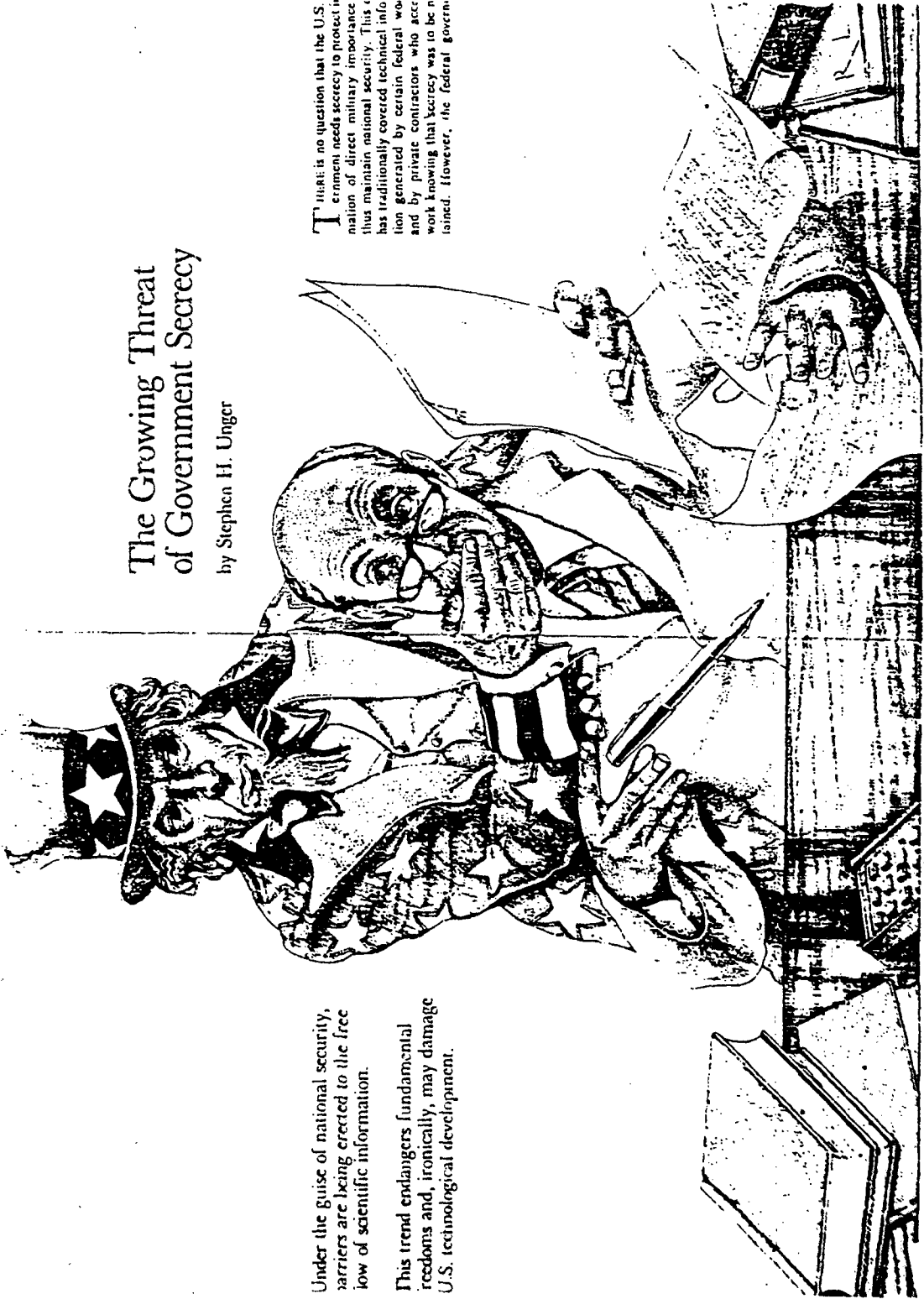
The Growing Threat of Government Secrecy

by Stephen H. Unger

Under the guise of national security, barriers are being erected to the free flow of scientific information.

This trend endangers fundamental freedoms and, ironically, may damage U.S. technological development.

THERE is no question that the U.S. Government needs secrecy to protect information of direct military importance and thus maintain national security. This has traditionally covered technical information generated by certain federal workers and by private contractors who accept work knowing that secrecy was to be maintained. However, the federal govern-



Clearly, any field closed to
foreign nationals would progress more slowly,
a result hardly likely to strengthen
national security.

has recently attempted to extend its control to include a much broader class of knowledge generated by non-governmental investigators whose projects are not directly related to national security. The underlying concept is that certain ideas may be declared secret regardless of their origin, and that publication of those ideas may be declared unlawful.

An important area in which government-imposed security is expanding is cryptography, the use of codes to render messages or data unintelligible to unauthorized parties. Until recently, codes were the domain of the military, intelligence services, the diplomatic corps, and puzzle enthusiasts. But the advent of nationwide digital communications, electronic funds transfer, and computer storage banks filled with data about individuals and businesses—as well as a growing concern about privacy in general—has expanded interest in cryptography. Major technological advances are now being made by researchers outside the group that long monopolized the field.

Suggestions from NSA

In 1977, the Institute of Electrical and Electronics Engineers (IEEE) scheduled a symposium at which several important papers in cryptography were to be presented. The research established a basis for developing powerful new encryption schemes using fundamental concepts of computer science. Examples of such schemes were included in the papers, which dealt not only with methods for concealing the contents of messages but also with solutions to the problem of authenticating authorship of received messages.

However, prior to the symposium a letter arrived at IEEE headquarters warning that the presentations might subject the authors and the IEEE to prosecution under the Arms Export Control Act of 1976. The letter was signed by an IEEE member, Joseph Meyer, who gave only his home address—but it soon emerged that Meyer was employed by the National Security Agency (NSA), whose functions are to intercept and decipher the communications of foreign governments and to safeguard the secret communications of the U.S. government. After due deliberation, the IEEE nervously went ahead with the symposium, although the papers of some graduate students were presented by their faculty advisors to ensure legal backing from their universities. No action was taken by the government. (It should be noted that Vice-Admiral B.R. Inman, then director of NSA, denies that NSA

attempted to suppress scholarly work in cryptography, citing a Senate committee finding that Meyer's letter to the IEEE was a personal initiative.)

Two other cases occurred that year. In October, the University of Wisconsin at Milwaukee filed a patent application (through an affiliated foundation) for an encryption device invented by George Davida, associate professor of electrical engineering and computer science. Six months later Davida received a letter from the U.S. Patent and Trademark Office informing him that if the principles of his invention were disclosed to anyone other than federal agents, he would be subject to a \$10,000 fine and two years in prison. The Invention and Secrecy Act of 1951 had been invoked—at the behest of NSA, it was later revealed. The Patent Office did not indicate how long the invention had to be kept secret, did not justify the secrecy order, and did not cite an appeals procedure.

About the same time, three engineers in Seattle—Carl Nicolai, William Raika, and David Miller—had filed for a patent on an inexpensive voice scrambler they planned to market, and they received a similar secrecy order. A furor arose around both cases as protests were filed and widely reported. In June 1978 the secrecy order involving Davida was rescinded, and the order on the scrambler was lifted the following October.

Yet another related sequence of events began in 1975, when NSA officials "suggested" to the National Science Foundation (NSF) that NSA had the sole authority to fund research in cryptography. NSF could find no legal basis to support such a proposal and rejected it. The matter was raised more formally in 1977, at which time NSF agreed to include NSA people among the reviewers of cryptography research proposals but did not surrender the right to fund such research at its own discretion.

The next step came in August 1980, when Leonard Adleman, a well-known researcher in cryptography at M.I.T. and the University of Southern California, was notified that NSF would not renew his research grant in full because certain parts of his proposal impinged on national security. Shortly thereafter, NSA said that it wanted to fund the research. Adleman rejected this suggestion and another storm of controversy ensued. Ultimately, an NSF internal review restored Adleman's entire grant.

The government's argument is that open research and publication in cryptography jeopardizes national security by making available to foreign governments encryption techniques that NSA would have difficul-

Foreign students who
return to their own countries constitute a significant
pool of goodwill toward the
United States.

ty breaking, calling to the attention of foreign governments the vulnerability of their current encryption methods, and revealing knowledge that might endanger the inviolability of codes used by the U.S. government. Although not openly admitted, a fourth motivation can be inferred—that private development of unbreakable codes would make it more difficult for the government to carry out surveillance of American citizens.

These points have been challenged on the grounds that the knowledge and abilities of people producing new ideas in cryptography are not an American monopoly. Also, the security of modern encryption systems does not depend on concealing the methodology but merely on keeping confidential “keys” necessary for decoding.

Another important argument flows from the U.S. dependence on electronic communications. In particular, financial transactions increasingly occur as digital messages. New types of fraud are based on the manipulation of data in computer storage banks or the interception and transformation of coded information, raising the possibility of major disruption by foreign agents and national economic chaos.

One defense against both small-scale and large-scale “data sabotage” would be the development and widespread deployment in the business community of powerful encryption and verification systems. Thus, national security could actually be impaired by excessive secrecy in cryptography research. This technology is far more important to the United States than to the Soviet Union, which lags far behind in the processing and transmission of digital data.

Campus Restrictions

Another manifestation of growing governmental secrecy is the effort to make American technology less accessible to foreign nationals. This includes federal demands that certain scientists from Communist countries be excluded from international conferences held in the United States, and proposals to exclude foreign students at American universities from research in key areas.

For example, early in 1981 the State Department informed Cornell University that a Hungarian engineer must limit his study of electronics to the classroom—no private seminars or discussions would be permitted, nor could he receive prepublication copies of research papers. Under these conditions, the visit was canceled. Another incident occurred at M.I.T.

when the State Department expressed concern that a Chinese physicist participating in an official exchange program might be exposed to information covered by export control regulations. And at Stanford University, the research program of several visiting Chinese scholars working in computer science was questioned. A letter from the State Department suggested that the program “emphasize academic as opposed to applied research.” There should be “no access to the design, construction, or maintenance data relevant to individual items of computer hardware,” the letter added. “There should be no access to design of microelectronics . . . This office should be advised prior to any visits to any industrial or research facilities.”

Such restrictions jeopardize academic freedom, since perhaps a third of all engineering and science graduate students at leading American universities are not U.S. citizens, and many faculty members are in the same category. (So are growing numbers of engineers and scientists in industry.) Their contributions can be gauged simply by leafing through scientific journals. Clearly, any field closed to foreign nationals would progress more slowly, a result hardly likely to strengthen the technological base of America’s national security. Also, foreign students who return to their own countries constitute a significant pool of goodwill toward the United States.

The Legislative Threat

In 1981 a bill was reintroduced in the House of Representatives that would alter the Arms Export Control Act. The bill—H.R. 109—would significantly strengthen controls on the export of information about items on the “U.S. Munitions List” established by that act. The list covers a broad spectrum of technology, including cryptography, computers, and communications equipment. And significantly, H.R. 109 proscribes *publication*: “Notwithstanding any other provision of law, information specified in such regulations, or materials revealing such information, shall not be published or disclosed unless the secretary of defense, in consultation with the secretary of state and the secretary of energy, determines that withholding thereof is contrary to the national interest.”

According to Representative George E. Brown, a member of the House Committee on Science and Technology, “This literally gives the secretary of defense unlimited powers to control, restrict, or forbid communications of any kind, technical or other-
(Continued on page 35)

U.S. Export Controls and Soviet Technology

by Thane Gustafson

ALARMED by the rapidly growing military strength of the Soviet Union, we wonder uncomfortably whether we have inadvertently contributed by exporting scientific knowledge and advanced technology. A decade ago, confidence in our military strength and the superiority of our civilian technology, and hopeful about the possibilities of cooperation with the Soviet Union, we began dismantling the virtual trade embargo maintained against Eastern Europe for nearly 20 years and set about expanding trade and contacts. We are far from that optimism now. And export controls are being reconsidered as part of a general rethinking of the premises of American policy toward the Soviet bloc.

The major weakness of the present system of controls, in the view of its critics, is that it allows important technology to slip through to our military competitors by paying too much attention to the export of products, and not enough to the control of broader technologies and management skills. Consequently, the most recent U.S. legislation—the Export Administration Act of 1979—mandates the development of a review procedure that will control classes of “critical technologies” rather than individual products. And the focus is on “active” mechanisms of transfer such as training agreements, long-term technical exchanges, extended workshops, and other apprenticeship arrangements.

Technology Roll-Call

However, there is serious question whether the critical-technologies approach will improve the export-control system. On the contrary, if we are not careful it could make the system more complex, cumbersome, and controver-

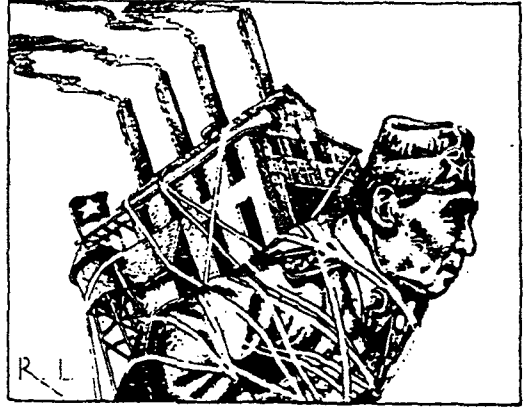
sial. The initial “Military Critical Technologies List,” issued in October 1980 by the Department of Defense, illustrates the danger: it contains a virtual roll-call of leading contemporary technologies. If this collection had automatically become the basis for the official Commodities Control List (as some urged during the debate over the 1979 Export Administration Act), the entire Department of Commerce would not have been large enough to administer the export-control program. Fortunately, the initial list had advisory status only and will certainly undergo refinement before becoming policy.

What exactly are we trying to prevent the Soviets from doing? In what ways does imported Western technology enable the Soviets to do the things we fear? Can export controls stop them or slow them down? These questions are central to any export-control policy, but there has been considerable confusion among American policymakers about all of them.

What is most critical about technology transfer is whether the receiving side is able to absorb the technology, diffuse it beyond one or two showcase locations, and build upon it to generate further technological advances of its own. Only then does technology transfer have its most lasting consequences.

In certain sectors (notably military) where Soviet technological skills are already high, the Soviets’ ability to learn from foreign technology is also high. Here, then, is a clear case for export controls. Something like the present system of case-by-case evaluation, aimed at preventing immediate military use of American technology by the Soviets, must and undoubtedly will continue.

But more pressing is what to do about the possibility that



the U.S. is giving away indirect military advantages through subtle channels that may call for more subtle defenses. The danger is not so much the possibility of sudden and disastrous giveaways, but rather that high-technology trade may help the Soviets gradually upgrade the traditionally neglected “civilian” industries that will provide broad, infrastructural support for new weapons systems.

In these lagging industrial areas in which most Soviet imports of foreign technology are concentrated, the Soviets’ record in absorbing and learning from it is poor. The reasons—similar to the ones that caused those areas to lag in the first place—lie deep in the political and economic structure of the country, and numerous reform measures in Soviet technology policy over the last decade have not altered them. Neither have high-technology imports visibly improved the Soviets’ ability to innovate: in some instances the opposite has happened.

Industrial managers in the Soviet Union are not rewarded for innovating; in fact, they may be penalized. Bonuses result from meeting

very tight production targets, and failure to meet those targets will jeopardize their careers. So the incentives lead managers to gear production toward established, “safe” technologies. Official efforts to mandate innovation by building targets into production plans have resulted in ruses such as “paper” innovation—inflated figures that look good on yearly reports but that do not reflect real gains in productivity.

Other problems in the civilian sector include a lack of experienced entrepreneurs who can “sell” the results of research to industry, a scarcity of new materials and supplies, and difficulty in obtaining “nonstandard” equipment from separate ministries. Innovation is further retarded by administrative and physical barriers—research and design institutes, pilot plants, and factories are seldom under the same roof and may even be in different administrative jurisdictions with conflicting outlooks and priorities. The flow of ideas, labor, and supplies across these institutional gaps is impeded by the fairly primitive state of copying and communications technology and other bureaucratic hurdles.

The effects of internal Soviet obstacles, in fact, dwarf those of the most stringent embargo the Western powers might devise. Consequently, so long as Soviet policies for technological innovation remain as ineffective as they are now, the claimed benefits of any expansion of U.S. export controls should be examined very carefully. Export controls can have important marginal political benefits, but they also have serious costs, and the task is to arrive at a balance.

Exports: A World View

Keep in mind that the U.S. is a small player in the total volume of Western high-technology exports to the Soviet Union. Our exports in 1979 amounted to \$183 million (\$270 million to Eastern Europe as a whole), about one-tenth the level of Soviet imports of advanced machinery and equipment from West Germany, France, and Japan combined. The chances of gaining much support from other countries for an expanded system of export controls are small and growing smaller, for among the nations conducting high-technology trade with the Soviet Union are not only NATO allies (whose reluctance to apply stiffer export controls is longstanding), but also countries such as Austria, Sweden, and Switzerland, which are unlikely to cooperate at all. Thus, we should not imagine that expansion of export controls would be free of serious political costs; indeed, such a move might be unenforceable at any acceptable cost.

History teaches that the control of technology transfer is at best a rear-guard action, achievable (and then only briefly) at the cost of regulations and secrecy that carry harmful side-effects. Balanc-

ing the political costs and benefits of export controls requires weighing their claimed effects against their costs in straining relations with allies and impeding the competitiveness of our exports.

Our first concern should be to remain good innovators ourselves. The case for export controls is strongest in areas in which the Soviet Union stands to make near-term military gains and in which the United States has a clear lead over other Western countries. As one moves outside this zone, toward technologies that afford the Soviets longer-term industrial gains and that are not areas of clear American superiority over the rest of the West, the benefits of export controls become more diffuse and uncertain, while the costs of trying to enforce them become greater. Thus, any widening of export controls outside the first range into the second should be undertaken only with the greatest care.

One issue I have not addressed is the use of embargoes or other selective controls on East-West trade as political levers to influence Soviet behavior in the international arena, or as symbolic statements of American positions. I do not necessarily quarrel with such uses of export controls; that is a question for the political process. But it is important to know whether export controls are effective in their stated aim (namely, to preserve military lead-times and national security), to clarify what those aims imply in operational terms, and to know the costs. □

Thane Gustafson, who received his Ph.D. in political science from Harvard, is a researcher in the Rand Corporation's Social Sciences Dept. and author of Reform in Soviet Politics (Cambridge University Press, 1981).

(Continued from page 33)

wise! This is so because the Munitions List is written in fairly broad language, and because of the customary leeway in the words 'in consultation with' and 'national interest.'

Indeed, the proposed bill would restrict the publication of a substantial portion of American research results, since prior approval would be required in areas such as lasers, computer circuitry technology, computational complexity (possibly related to cryptography), and high-energy particle beams. An extraordinary aspect of H.R. 109 is that it places the burden of proof on those who wish to publish, rather than requiring the government to make a case against publication. And scientists must show not only that publication would not be damaging but also that *failure to publish* would be "contrary to the national interest."

H.R. 109 has been referred to the Subcommittee on International Security and Scientific Affairs of the House Foreign Affairs Committee. Comments have been requested from the Departments of Defense, State, Energy, and Commerce, but no hearings have yet been scheduled.

The council of the Association for Computing Machinery approved a strongly worded resolution condemning H.R. 109 and its underlying philosophy. This resolution was recently endorsed by the IEEE Computer Society. Although such an extreme law as H.R. 109 may be unlikely to pass, the fact that it was introduced in two successive sessions of Congress makes this a serious matter. That the bill's sponsor is Charles E. Bennett, ranking Democrat on the Armed Services Committee, adds further weight.

Does Secrecy Promote Security?

U.S. military strength has long rested on the country's powerful industrial structure and American technological prowess. However, U.S. scientific supremacy has recently come into question in a number of important fields, both commercial and military. For example, Japan and West Germany have surpassed American firms in certain aspects of microelectronics. More worrisome, the Soviet Union—once nearly a decade behind in electronics—has closed the gap to perhaps five years. Meanwhile, the performance of American industry in the area of military hardware has flagged. Failures to meet cost estimates and delivery dates, as well as operational unreliability, are evident in America's latest efforts to develop new tanks, military aircraft, and command-and-control systems.

Of Bubbles, Bombs, and Batteries: Secrecy Snafus

Advocates of increased secrecy contend that our relative position will be further eroded if we continue to give away the results of our research and development efforts. At the very least, they argue, we should delay for a few years the dissemination of information directly applicable to production processes.

While the case for restricting the outflow of technical and scientific information is relatively straightforward, counterarguments are rather involved and diverse. The first directly challenges the argument that national security is enhanced by increased secrecy. Virtually all methods for inhibiting the international flow of scientific and technical information require restrictions on its domestic circulation. For example, there is no practical way of keeping an article published in an American journal from reaching potential rivals overseas. Ideas to be kept from crossing the ocean must also be kept out of general-circulation publications, and hence would not be accessible to most Americans.

Such a restrictive policy would result in the duplication of scientific research and interfere with the interactive process vital to advances in science and engineering. Our large technological lead was built without significant information barriers, and no increase in the outflow of technical know-how appears to account for the recent reduction of that lead.

Requiring clearance before a paper can be presented at a meeting or published can only discourage people from working in fields covered by such regulations. This is particularly true at universities, where publication is important and researchers are free to choose the problems they tackle.

Expanded secrecy and free enterprise also conflict, as evidenced by the government's move to suppress commercialization of the voice scrambler developed by the Seattle inventors. And broadening constraints on the transfer of technical information by foreign nationals has obvious negative implications for international trade.

Openness has always been a leading attribute of American society; we take for granted the lack of censorship on what may be said or printed, even though these traditions have sometimes been violated. New barriers to scientific communication—especially prior restraint on publication and speech—not only raise questions about First Amendment rights but detract from the example of openness that America sets for the world. Such barriers would also damage

(Continued on page 38)

MAGNETIC bubble devices are computer memory elements now beginning to find use in commercial equipment. They offer a good combination of speed and price—but are not considered unusually important scientifically, and there seems little reason to view bubble memory as having great military significance.

In February 1980, the American Vacuum Society (AVS) held a small international meeting on bubble memory in Santa Barbara. Five working days before the meeting, the Commerce Department informed AVS that the conference was covered by export regulations and that "oral exchanges of information in the U.S. with foreign nationals constitute export of technical data." Such export would require a license when the destination was Eastern Europe. Failure to comply would subject conference organizers to large fines and imprisonment for up to 10 years. Foreign attendees would be required to provide written assurance that data would not be passed on to Eastern Europe.

The State Department quickly became involved and, at its suggestion, AVS rescinded its invitations to Poles, Hungarians, and Russians. The Commerce and State Departments conflicted as to whether three Chinese scientists who arrived during the controversy should be excluded.

After the approximately 30 foreign participants signed agreements not to "re-export" what they learned to any of 18 nations (including China), the meeting began. And on opening day, the Commerce Department finally agreed to allow the Chinese to attend, provided they signed the agreement with China deleted from the list. A government official later explained that

such restrictive regulations are not intended to interfere with the exchange of basic scientific information, but only to block the outflow of "information that will enable somebody to build something."

That same month a much larger meeting in San Diego caused problems. Sponsored by the Optical Society of America and the Institute for Electrical and Electronics Engineers, its title was "Conference on Lasers and Electro-Optical Systems and the Topical Meeting on Inertial Confinement Fusion." Here the State Department intervened, notifying the organizers that eight Russians would be denied visas, including one member of the program subcommittee. A Russian post-doctoral researcher at the University of Texas, coauthor of a paper to be presented, was also denied permission to attend. (No restrictions were placed on the more than 300 scientists from other nations.)

The State Department explained that much equipment was to be exhibited at the meeting, and that prohibiting Russian participation was a reaction to the Soviet invasion of Afghanistan. However, inertial-confinement fusion is probably the area in which the U.S. has benefited most from its longstanding scientific cooperation with the Soviet Union.

Secrecy and the Atom

In 1976, L.I. Rudakov, a prominent Soviet physicist, toured the U.S. to lecture on his work in electron-beam fusion. This research has important application in controlled thermonuclear fusion for energy production but also indirectly relates to hydrogen bombs. After each lecture, facility officials were notified by the Energy Research and De-



velopment Administration (now Department of Energy) that the subject was classified and the ideas presented should not be disseminated. Since the reasons for classifying material are themselves secret, there has been no explanation of why the U.S. government would want to classify work that the Soviets themselves are willing to report.

Perhaps an even more significant incident occurred in 1979, involving not a scientist's work but a journalist's article written for a monthly political magazine based in Madison, Wis. *The Progress-*

sive was ready to publish Howard Morland's article "The H-Bomb Secret: How We Got It, Why We're Telling It." When DOE officials read a preliminary copy of the manuscript in early March, the agency declared that it contained "restricted data" and asked the magazine to revise it. The editor refused and DOE obtained a temporary restraining order from a U.S. district court in Wisconsin. Several weeks later, following a closed-court hearing, the same judge issued a preliminary injunction against publication. This was appealed

to a circuit court, and hearings were held that September.

The article provoking this commotion was based on material that Morland assembled from the open literature, including declassified government documents: the government never claimed that any of this information had been obtained illegally. The basis for the injunction was that the information was presented in a manner that would help other nations construct hydrogen bombs. This was the first time in American history that prior restraint was exercised against a publication on grounds of national security—with the sole exception of the 1971 Pentagon Papers, and the Supreme Court dissolved that order within a few days.

The Progressive case ended abruptly prior to completion of the appeal process when a Madison newspaper published a similar article. The Justice Department announced that this rendered the case moot.

An interesting sidelight was the way the government used its power to classify or declassify information to hamper *The Progressive* in its legal battle and to manipulate what information was released to the media. For example, security restrictions made it difficult for the magazine to gather evidence supporting its contention that the article would not significantly increase the knowledge of anyone already capable of using the information. And when the magazine did obtain supporting affidavits from experts with access to secret information, their statements were promptly classified.

When several Argonne National Laboratory scientists wrote to Senator John Glenn about the misuse of DOE's security classification procedures, their letter was classified. On the other hand, testi-

mony supporting the government's case was made public, even though it violated security regulations by commenting on the accuracy of the Morland article. Subsequently, Livermore Laboratory physicist Hugh DeWitt, who provided an affidavit supporting the magazine, was accused by DOE of violating security procedures. DeWitt fought back with support from his congressman, several scientific societies, and his union. All charges were eventually dropped.

Cloaked Creativity

Secrecy orders on inventions—which block the granting of patents and prohibit the inventor from disclosing the invention to anyone else—are issued by the commissioner of patents and trademarks. In fiscal 1979, about 5 percent of the over 100,000 patent applications were routed by the Patent Office for review by defense agencies. This resulted in 243 secrecy orders, about 40 of which pertained to nonclassified work. In addition, about 3,300 existing orders were renewed.

Most secrecy orders cover inventions developed by government agencies or contractors working on military-related matters and protect devices obviously connected with national security, such as missile-control apparatus. But military agencies have also requested secrecy in other cases. For example, in 1980 Rohm and Hass tried to patent an improved electrochemical battery, but a secrecy order was issued at the behest of the U.S. Army. The research had been carried out for commercial purposes with company funds, but activity stopped for about six months until government officials were persuaded to rescind the order.—S.H.U. □

Virtually all methods for
inhibiting the international flow of scientific and technical
information require restrictions on its
domestic circulation.

one of the few strands of international cooperation—that which links scientists and engineers across national boundaries.

Rules and Regulations

The International Traffic in Arms Regulations (ITAR) were developed as part of the Mutual Security Act of 1954, largely superseded by the Arms Export Control Act of 1976. Administered by the State Department, ITAR regulates the export of military hardware. "Technical data" are defined to include unclassified information useful in "the design, production, manufacture, repair, overhaul, processing, engineering, development, operation, maintenance or reconstruction of . . . implements of war on the U.S. Munitions List," or "any technology that advances the state-of-the-art or establishes a new art in any area of significant military applicability." The U.S. Munitions List is over seven pages long, including all the obvious items such as automatic weapons, torpedos, and missile guidance systems. It also includes electronic equipment for space flight, aerial cameras, energy conversion devices designed or modified for military equipment, speech scramblers, "privacy devices," computers, and communications equipment designed for military use.

This broad definition leads to problems. For example, a new development in metallurgy could easily be considered applicable to the development of military armor plate. A conference presentation detailing a new technique for improving signal detection in the presence of noise would be covered as relevant to the design of military radar systems. And since ITAR puts the burden for obtaining government approval "on the person or company seeking publication," one could reasonably say that a substantial portion of the engineering and scientific community has long been violating the law and is subject to criminal penalties: up to two years in prison and a \$25,000 fine for each violation. Defense Department official Larry Sumney recently said that "the ITAR, if enforced to the letter, would cover virtually everything done in the United States. But people understand they are written very generally." He added that they will not be capriciously enforced, and no prosecutions have yet occurred for the publication of scientific or technical articles.

A 1978 Justice Department memorandum to presidential science advisor Frank Press (signed by Assistant Attorney General John M. Harmon) concluded that "the existing provisions of ITAR are unconstitu-

tional insofar as they establish a prior restraint in disclosure of cryptographic ideas and information developed by scientists and mathematicians in the private sector." It also indicated uncertainty as to the adequacy of the legislative authority for the technical data provisions of ITAR.

In December 1980, the government proposed a revision of ITAR that narrows somewhat the definition of technical data (the part about advancing the state-of-the-art was deleted) and weakens, perhaps effectively eliminating, the requirement on obtaining clearance prior to domestic publication. However, the revision does not appear to ease restraints on presentations at technical meetings or other contacts with foreign nationals.

Still More Regulations

The Department of Commerce, under authority of the Export Administration Act of 1979, administers the Export Administration Regulations (EAR), which include a section on technical data. The EAR definition of technical data, a bit narrower than the ITAR definition, applies only to "design, manufacture, utilization, or reconstruction." But it also is broader in that it applies to all "articles and materials" rather than just weapons-related items. Those items on the Commodity Control List may not be exported to certain nations without first obtaining special export licenses.

However, a general license exempts data "generally available to the public in any form." This includes items that can be purchased at nominal cost, information available in public libraries, or knowledge released at open conferences. The regulations are designed to control the outflow of manufacturing details without unduly impeding commerce.

A group of government agencies, led by the Department of Defense, is now compiling a "Military Critical Technologies List" (MCTL), as mandated by the 1979 Export Administration Act. The goal is to identify the technological elements essential to an advanced military capability, and MCTL will be used to revise the Commodity Control List. The kind of basic scientific knowledge developed in universities will be excluded, but there is a considerable grey area between what might be considered industrial know-how and what is advanced engineering research. This is particularly true in microelectronics, where there is great overlap between research at universities and in industry.

Such barriers would also
damage one of the few strands of international cooperation:
that which links scientists and engineers across
national boundaries.

Since 1917 the government has been legally able to order that inventions be kept secret on grounds of national security. This restriction originally applied only during wartime. Later legislation removed this restriction but required that such orders be reviewed annually unless the president has declared a national emergency, in which case the orders remain in effect until six months after the emergency ends. (The emergency proclaimed by President Truman in December 1950, during the Korean War, lasted for 28 years.)

Secrecy orders are issued by the commissioner of patents and trademarks when the head of a defense agency issues an opinion that disclosure "would be detrimental to the national security." No such order has ever been subjected to judicial review, nor has there ever been a judicial test on First Amendment grounds.

Secrecy orders may be issued even if the Patent Office does not consider the invention patentable or if the patent application is withdrawn. Inventors may appeal to the secretary of commerce after petitions to the sponsoring defense agency have been denied. The inventors are entitled to seek compensation for damages, but this right has rarely been exercised successfully. Only 29 claims were filed between 1945 and 1980 (about one per thousand orders): 9 have been settled, 10 denied, and the rest are still pending. Litigation is generally quite lengthy: in 1977, General Electric finally won a suit concerning a World War II radar invention.

Special secrecy rules apply to atomic energy and are administered by the Department of Energy (DOE). Authorization stems from the Atomic Energy Act (the latest version was passed in 1954), intended to protect American security in the nuclear area, inhibit the international proliferation of nuclear weapons, and promote the use of atomic energy for peaceful purposes. Clearly, a delicate balance must be achieved.

For example, many areas of knowledge are applicable to both weaponry and nonmilitary purposes. Technology for producing fissionable materials could be used in operating nuclear reactors or building atomic bombs, and DOE can declare secret any information it considers "relevant to national security matters." Of course, the growth of the nuclear energy industry worldwide has greatly enhanced the amount of openly available information.

Another secrecy-related problem pertains to the source of knowledge. Any person making an invention

or discovery in the field of atomic energy must file a report with DOE within six months, unless a patent application has been filed. The DOE may rule that the invention contains restricted data, thus acquiring control over its dissemination. If a patent application is filed, the Patent Office must notify DOE, which may then request a secrecy order.

Secrecy Solutions

An outgrowth of the cryptography controversy was the formation in 1980 of the "Public Cryptography Study Group" (PCSG), assembled by the American Council on Education and funded by NSF. The nine-member group included mathematicians and computer scientists nominated by various professional societies, some university administrators, and the general counsel of NSA. The group's goal was to satisfy NSA's concerns about the publication of cryptography research without unduly hampering such research or impairing First Amendment rights.

The PCSG first considered a mandatory system, backed by NSA, that would require all papers dealing with cryptography (as defined by NSA) to be submitted to NSA for prepublication censorship. The burden of proof would be on the government, judicial review would be provided by a special court acting under "suitable security precautions," and compensation would be provided for economic losses resulting from the constraints.

This proposal was rejected, partly because the group felt it had not been able to assess the need for secrecy. (NSA said it could not present its case fully unless the group applied for security clearance, which it did not do.) Another reason was the negative impact the NSA proposal might have on cryptography, harming individual and commercial privacy as well as foreign trade. The PCSG was also unable to define what should be kept secret with sufficient precision to satisfy what it regarded as constitutional requirements. Finally, the group felt that a compulsory system would not be as practical as a voluntary system, which would more likely gain cooperation from researchers.

The PCSG eventually recommended that a system be established, on a trial basis, in which NSA would invite authors to submit cryptography manuscripts for prior review. NSA would determine the areas to be covered in consultation with appropriate technical societies, excluding fields such as "general mathematics" (Continued on page 84)

Unger/Continued from page 39

ics, engineering, computer science or statistics, and basic theoretical research." Manuscripts would be returned promptly to the authors with explanations "to the extent feasible of proposed changes, deletions, or delays in publication, if any." A disagreeing author could request a review by a standing advisory committee, with two members appointed by the NSA director and three by the president's science advisor. The entire process would be voluntary, with neither authors nor publishers required to participate or comply with any proposed restrictions.

This proposal was accepted by all members of the PCSG except George Davida (nominee of the IEEE Computer Society), who wrote a minority report arguing against any restraints. Among his many objections is the difficulty of distinguishing between basic research and knowledge directly applicable to actual systems. As an example, he points out that one new encryption scheme, already used in a safeguard system at a nuclear power facility, depends on the difficulty of factoring very large numbers. However, progress has been made recently toward developing efficient factoring methods. Should this field, one of the oldest in mathematics, now be regarded

as falling within the regulated category?

Davida also expressed concern that a voluntary system could be a first step toward a compulsory system, and that the PCSG report could be used to validate NSA's argument about the necessity for controlling cryptography research. He concluded that control would serve no useful purpose, and that "NSA can perform its mission the old-fashioned way: *stay ahead of the others.*"

The only other cryptography researcher on the PCSG—Martin Hellman, an electrical engineer at Stanford and a leader in the field—supported the proposal. Although sympathizing with Davida's concerns, Hellman said he felt that NSA had been acting more reasonably of late, and he wished to encourage this trend by responding positively. He had even begun sending prepublication copies of his papers to NSA (without promising to abide by requests not to publish). The thrust of his argument is that the system would test the validity of NSA's position by presenting its arguments to the advisory committee. And he worried that if what he regards as NSA's more reasonable attitude is not rewarded, the agency will revert to its earlier position.

The IEEE has recently taken the position that its publication procedures place the burden of securing appropriate indus-

trial and governmental clearances on the authors, hence it is unlikely to involve itself directly in the voluntary review system proposed by the PCSG. The Association for Computing Machinery will probably adopt a similar stance.

Enough Is Enough

Although there may be disagreement over how much secrecy is justified, there is little evidence for the view that the government has not been sufficiently secretive. On the contrary, there are all too many indications that secrecy, particularly in the name of national security, has been abused by government officials.

The futility of trying to suppress scientific knowledge is illustrated by an occurrence in the early 1940s. Prior to the Manhattan project, American scientists agreed not to publish research on nuclear fission to avoid revealing anything that would encourage other nations to develop atomic bombs. Observing this sudden publication halt, G.N. Flyorov, a young Soviet physicist, deduced that the United States must have embarked on a secret nuclear project and urged his government to proceed immediately in the same direction.

Apart from damaging our technological competence, prior censorship, even in a few specialized fields, would set dangerous

MIT SUMMER SESSION 1982

The 1982 Summer Session at MIT includes programs in:

Chemical Engineering
Computer Related Studies
Electrical Engineering
Materials Science and Engineering
Mechanical Engineering
Nuclear Engineering
Ocean Engineering
Engineering and Applied Science
Health and Safety
Nutrition and Food Science
Management
Finance and Investment
International Affairs
Technical Writing and Editing
Decision and Risk Analysis

The Summer Session of 1982 will be the thirty-third in which MIT has presented Special Summer Programs for professional men and women to keep pace with developments in their fields.

Further details of content, participating staff, special lectures, living accommodations, and registration, together with an application blank for admission, will be available for each program by March 1, 1982. Address all inquiries to:

Director of Summer Session
Room E19356
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

precedents. Freedom of speech and freedom of the press are too precious to be jeopardized by what can only be described as loss of nerve.

Censorship should not be encouraged in any way. Even such an apparently innocuous voluntary system as the PCSC proposal is dangerous, establishing censorship machinery and accustoming people to its very existence. This makes the next step easier: compulsory review. The threat of expanding government secrecy in technology merits the serious attention of scientists and engineers—both as professionals and as citizens—and should be strongly resisted.

Further Reading

Choh, Mary M., "The Progressive Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls." *George Washington Law Review* 48.2 (January 1980): 163-210.

Diffie and Hellman, "Privacy and Authentication: An Introduction to Cryptography." *Proceedings of IEEE* 61.3 (March 1973): 397-427.

Kahn, David, *The Codebreakers*. New York: Macmillan, 1967.

U.S. Congress, House of Representatives Committee on Government Operations, "The Government's Classification of Private Ideas." House Report no. 96-1540, December 1980.

Wise, David, *The Politics of Lying: Government Deception, Secrecy, and Power*. New York: Random House, 1973.

Stephen H. Unger earned a Ph.D. in electrical engineering at M.I.T. and is currently a professor of computer science at Columbia University. His book, *Controlling Technology: Ethics and the Responsible Engineer*, will be published this spring (Holt, Rinehart, and Winston). This article is adapted from a paper prepared for the Committee on Scientific Freedom and Responsibility of the American Association for the Advancement of Science.

Letters/continued from p. 4

tists who will move this society into a "golden age" of advancement.
Ken McGhee
Washington, D.C.

Samuel Florman asserts that we have the freedom to run technology rather than be run by it. Yet he concludes by saying, "For all our apprehensions, we have no choice but to press ahead . . . We simply cannot stop while there are masses to feed and diseases to conquer, seas to explore and heavens to survey." If we cannot stop, then we have no freedom. Perhaps Mr. Florman is only being rhetorical; being tragic often means being blind.
David Lukens
Evanston, Ill.

It is astounding that Samuel Florman fails to examine the public institutions that generate new technologies and thereby shape

February/March 1982

their character. Lotty speculations by Shakespeare, Hegel, and George Steiner offer little insight into why people fear technology. There are structural and institutional reasons why Ford Pintos are dangerous in rear-end crashes and why job automation can make work less enjoyable and even oppressive. Coaxing the scaredy cats who worry about "out-of-control" technology out of their "immaturity" will take more than platitudes.

David Bollier
Washington, D.C.

Mr. Florman responds:

Dismay over public institutions is an appropriate companion to fear of technology. In blaming amorphous evil forces, Mr. Bollier avoids confronting real problems to which there are no easy answers. People want cars that are cheap, snappy-looking, and fuel-efficient; they want to enjoy the wondrous benefits of electronic technologies and use the splendid products that flow from automated factories. But people must face up to the consequences (not all pleasant) of their desires. Refusal to do so is not political sophistication it is, indeed, immaturity.

Not Needs but Desires

John Matril states in his "Engineering the Ivory Tower" (October, page 2) that "by definition engineering is science applied to the needs of humanity." This is the conventional definition of engineering, but not the definition of engineering as it really is.

Engineering is not limited to applied sciences; it includes the great body of information obtained by testing and experience. A good definition of engineering is "the use of forces and materials of nature to satisfy the desires of humanity." Young engineers who believe that science is the sole source of their knowledge are in for a rude awakening. Certainly the fraction of engineering knowledge common to science is steadily increasing, but it is still much less than 100 percent.
William M. Brobeck
Berkeley, Calif.

Cottage Computer Industry

After reading Alvin Toffler's *The Third Wave*, I was very interested in Robert Cowen's comments in "Cottage Computing: Glorifying the Trivial" (November/December, page 6). Mr. Toffler points out the schism between home life and business life in industrial civilizations. Other commentators have noted that the determined exclusion of children and adolescents from business life has alienated one generation from the next. I take exception to Mr. Cowen's view. The microcomputer is a viable alternative to the large-scale disruption of family life caused by centralized processing facilities.

John T. Wilson
Somerville, Mass.

Upcoming in our April issue:

What to Do Before the Oil Runs Dry:

An energy futurist explains the Washington and California scenes.

Avoiding the Risks of Risk Assessment:

A guide to the use of a powerful but limited tool.

Computer Crime:

How sophisticated are thieves, hackers, and profits to the way you do business?

Telecommuting:

To work at home and at the office simultaneously.

Why is it foolish to use a computer to do things we already do with less expense and effort? I'm not a computer nut, but I appreciate its application in my home and business. My Apple provides me with cash-flow information, investment analysis, budgets, and other business tasks in about one-fifth the time it takes my company computer to perform these functions. I don't know much about programming but I'm learning, and what is more important, my children are learning, too.

Thomas N. Herr
Minneapolis, Minn.

Solution to the CO2 Problem

L.B. Lave's "A More Feasible Social Response" (November/December, page 22) seems unduly pessimistic about government initiative in dealing with atmospheric CO2 buildup. A proper strategy would be to eschew price controls, allow fossil fuel to be priced by the market, and prevent externalization of costs by users through rigorous environmental-protection regulations such as smog control. Penalties on fossil-fuel use will make alternative energy sources economically attractive sooner.
Kenneth Turner
Sacramento, Calif.

Scientific Freedom: Where Does
Congress Stand?

Robert L. Park

American Physical Society

Office of Public Affairs

Washington D.C.

and

University of Maryland

College Park, Maryland

In the course of Pericles' Funeral Oration, Thucydides remarks that ". . . there is a great difference between us and our opponents in our attitude toward military security. Our city is open to the world, we have no periodical deportations in order to prevent people observing or finding out secrets which might be of military advantage to the enemy. This is because we rely, not on secret weapons, but on our own real courage and loyalty." Athens, of course, eventually lost the Peloponnesian war.

Few people in today's world would argue with the necessity for governments to guard closely certain information. It is, however, an uncomfortable necessity for a democracy. Official secrecy is more vulnerable to abuse than perhaps any other instrument of government. Behind its cloak erroneous information goes unchallenged, the foolishness of government officials remains concealed from the public, and information is selectively leaked for political advantage. In seeking the correct balance between security and openness, therefore, the consistent trend for more than three decades has been to relax the use of classification.

In early April of 1982, this trend was reversed. The Reagan Administration issued Executive Order 12356 on Security Classification Policy and Procedures, which significantly expanded

the categories of classifiable information and made it possible for the first time to reclassify information that had been previously declassified. The directive prohibited the classification of basic scientific research not "clearly related to the national security," but implicit in that prohibition is the assumption that some basic scientific information is related to national security and should be classified.

The futility of attempting permanently to lock up scientific and technical information is, nevertheless, generally acknowledged by those with the responsibility for guarding our security. Our opponents have scientists and engineers of their own and they will in time develop the same information that we have, without violating our security. As an alternative, therefore, much of the emphasis in recent years has been on attempts to restrict the flow of information to our adversaries by means that fall short of actual classification. The object is simply to slow down the acquisition of our technology by our opponents.

The issue is not a simple one. We are all concerned when developments paid for by the American taxpayer are acquired at little cost by our opponents. In recent years the Soviets have acquired our technology at a rate that some regard as alarming. To stem this flow (it has been called a "hemorrhage"), the government has taken or is contemplating measures that could prove harmful to the very system that has given us our lead in technology. Any attempt to restrict the flow of information to our adversaries must inevitably impede our own progress.

The National Academy of Sciences constituted the Panel on

Scientific Communications and National Security, under the chairmanship of Dale R. Corson, to address this complex and critical issue. Their thoughtful report, Scientific Communication and National Security, issued in September 1982, was generally applauded by people on all sides of the issue.¹ The principal recommendation of the report was that national security is best served by a policy that stresses scientific and technical accomplishment rather than curbs on the free flow of information. The report did acknowledge, however, that a narrow gray area might exist that does not warrant outright classification but would justify some restraints on dissemination. The criteria for identifying technologies in this gray area were carefully spelled out. The Panel recommended that no restriction of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involved a technology meeting all the following criteria:

- o The technology is developing rapidly, and the time from basic science to application is short;
- o The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;
- o Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and
- o The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours.

To a scientist it may have seemed that the matter was

settled. A problem had been identified, a capable group of investigators had examined it, and a solution had been proposed that everyone seemed to agree was correct. What then has happened in the period since the report of the Corson panel was issued? This is the subject of a very thorough and careful account by Mitchel B. Wallerstein in a recent issue of Science.² His report is much too extensive to summarize here. It may, however, be worthwhile to list some of the conclusions:

- o The government has not acted in a manner compatible with the major Corson report principles.
- o There is a lack of effective government-wide coordination in this area.
- o There has been little progress toward an improved understanding of the technology leakage problem and the effects of control measures.
- o Continuing incidents of government interference in international scientific conferences are a source of acrimony.
- o The open communication of unclassified scientific information is a small part of the overall problem of unwanted technology transfer.

This is a troubling assessment. Science and government, which for more than four decades have formed a highly successful partnership, view each other with increasing suspicion and impatience. Where should we look for a resolution to these problems? It will be the purpose of this article to review current legislative actions as they relate to the issue of

scientific communication and national security.

The Export Administration Act

The Export Administration Act of 1979, which is administered by the Commerce Department through the Export Administration Regulations, is the principal statutory authority for the control of scientific communication. The Act was officially scheduled to expire on September 30, 1983. The President signed a bill extending its provisions for fourteen days, but when at the end of that period Congress still had not acted to pass new export administration legislation, the President invoked his Emergency Powers to extend the effect of the Act indefinitely. As a measure of the strong feelings held by some members of the Administration on this issue, Under Secretary of Commerce Lionel Olmer issued a stern warning against taking advantage of a hiatus of a single weekend between the expiration of the Act and the issuance of the President's emergency executive order.

Finally this spring legislation was reported out of committee in both Houses of Congress. The two bills, H.R.3231 and S.979, were quite similar and both contained language protecting scientific communication that had been recommended by the Association of American Universities.

It is the policy of the United States to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and other scholars freely to communicate their research findings by means of publication, teaching, conferences,

and other forms of scholarly exchange.

However, a Floor Amendment to the Senate version introduced by Senator Jesse Helms (R-NC), changed the provision to read:

It is the policy of the United States to sustain vigorous scientific enterprise. To do so involves sustaining the ability of scientists and other scholars freely to communicate their non-sensitive research findings by means of publication, teaching, conferences, and other forms of scholarly exchange.

You will note that the words "involves sustaining" have been substituted for "requires protecting." And more significantly, the word "non-sensitive" has been inserted before "research." Whereas it may be argued that "involves sustaining" is less firm than "requires protecting," the real damage of the Helms Amendment is the insertion of the word "non-sensitive." "Sensitive research" is the term that the Department of Defense has adopted to describe the gray area of the Corson report. The gray area as conceived by the Corson panel was to be very narrow (perhaps no more than five technologies). Unfortunately the DoD has shown a tendency to expand the gray area to encompass its Militarily Critical Technical List (MCTL). The DoD's proposed restraints on the dissemination of sensitive information go well beyond what was envisioned by the Corson panel. Indeed it can be argued that "sensitive" represents a new level of classification, but a level with fewer restraints on its imposition than the conventional levels of classification. It is quite conceivable that the language in the Senate version could, in fact, encourage the

increased application of export control restrictions on open scientific communication.

A Joint Conference Committee of Congress has been named to resolve these and other differences that emerged in the final form of the two bills. It is too early to predict what the outcome of that Conference will be, but from the standpoint of the academic and industrial research communities, it would be better to delete the entire paragraph from the declaration of policy than to use the Senate version.

A very distinct possibility, of course, is that the two houses of Congress will be unable to resolve their differences. In that event, it is probable that Congress will extend the provisions of the Export Control Act of 1979, since they are not likely to leave it under the control of the President's Emergency Powers.

The Freedom of Information Act

There is, of course, a whole zoo of legislative acts, government regulations, and administrative directives that have at least the potential to restrict the flow of scientific information. One of the most disturbing is an amendment to the Defense Authorization Act of 1984 that authorizes the Secretary of Defense to withhold unclassified technical information in the possession of the Department of Defense from the provisions of the Freedom of Information Act if it would be subject to export control. Moreover, a report by the DoD Subcommittee on Publications to the Steering Committee on National Security and

Technology Transfer, dated November 9, 1983, recommends that the Department of Defense serve as a repository for other agencies wishing to shield documents from the F.O.I.A. This would appear to go well beyond the intent of Congress. The Freedom of Information Act was, of course, intended to make all unclassified government documents available to the public, with a few careful exceptions involving such things as sensitive personnel records.

In a recent editorial in Physics Today, Robert Marshak, past President of The American Physical Society, wrote "Americans have never been comfortable with secrecy. It is too apparent that oppressive governments have the most to conceal. We have prided ourselves on the openness of our society and when even our constitutional safeguards seemed inadequate to insure that openness, we invented the Freedom of Information Act, a totally unprecedented testament to the self-confidence of a nation."³ It would be unfortunate if this act of openness in government were to be circumscribed by amendments aimed at export control.

National Security Decision Directive 84

All of this has taken place in a general atmosphere of increased secrecy in government. Government actions which are not aimed solely at scientific communication could nevertheless have a significant effect on the health of science. Perhaps the most notorious example of such an action is National Security Decision Directive 84 on safeguarding national security information. The Directive authorized three kinds of actions to prevent

unauthorized leaks of security information:

- o All government employees and contractors with access to Sensitive Compartments Information would be required to sign a contract agreeing to prepublication review of their writings for life. This would involve some 128,000 government employees.
- o The massive use of polygraph examinations was authorized to locate the source of leaks and to identify those government employees who might be expected to leak information. As many as one half million government employees would be subject to polygraph examination.
- o Contacts between those who have access to highly classified information and the media were to be restricted, although the mechanism for this was never spelled out.

While the reliance on the polygraph seems strange in the light of recent studies attacking its validity,⁴ the most serious consequence of the Directive from the perspective of the science community is the disincentive for scientists to serve in government. Most of our leading scientists and engineers have at some point in their careers served the government in positions that required access to highly classified information. It is not clear how many would undertake such service if the consequence involved censorship of their writings for life.

Following hearings before the Senate Government Affairs Committee, Senators Charles Mathias (R-MD) and Thomas Eagleton

(D-MO) introduced an amendment in the Senate to the State Department Authorization Bill barring the lifetime censorship provisions of the prior review contract, except for CIA and NSA employees. The amendment carried easily.

In the House, hearings were held by the Committee on Government Operations Subcommittee on Legislation on the National Security chaired by Jack Brooks (D-TX). Brooks later introduced the Federal Polygraph Limitation and Anti-censorship Act of 1984. Faced with this mounting criticism from Congress, the White House suspended implementation of NSDD 84 but stopped short of actually withdrawing it.

The record of Congress on issues of freedom of scientific communication is murky. What is clear is that the science community has failed to convince to Congress or the Administration of the essential role of free communication in scientific or technical progress. The exchange of results and ideas is such a natural part of scientific research that few scientists are able to trace the origins of their inspirations. The task is now to explain that somewhat wild process to non-scientists.

References

1. Committee on Sciences, Engineering, and Public Policy, National Academy of Sciences, National Academy of Engineering, Institute of Medicine, Scientific Communications and National Security (National Academy Press: Washington, D.C., 1982).
2. Mitchel B. Wallerstein, "Scientific Communication and National Security in 1984" Science, 224 (1984), 460-466.
3. Robert E. Marshak, "The Peril of Curbing Scientific Freedom," Physics Today, 37 (Jan. 1984), 192.
4. Scientific Validity of Polygraph Testing: A Research Review and Evaluation (Office of Technology Assessment: Washington, D.C., 1983); D. T. Lykken, "Polygraphic Interrogation," Nature, 307 (1984), 681-684.



Science, Technology, & Human Values

Contents

- | | |
|----------------------------------------------------------------------------------------|---------------------------|
| Beyond "Bad Science": Skeptical Reflections on the Value-Freedom of Scientific Inquiry | Helen Longino |
| The NAS Report on Scientific Communication and National Security: Excerpts | |
| Commentary on the NAS Report | Rosemary Chalk |
| Conference Report: Engineering Ethics | Rachelle Hollander |
| The Terrible Temptation of the Technological Fix | Jeff Douthwaite |

Also in this issue:
Responses & Reconsiderations
Bibliography
News Items
Meetings Calendar

ISSN 0162-2439

Published by

John Wiley & Sons

New York • Chichester • Brisbane • Toronto • Singapore

Cosponsored by the John F. Kennedy School of Government, Harvard University, and the Program in Science, Technology, and Society, Massachusetts Institute of Technology

Commentary on the NAS Report

Rosemary Chalk

The National Academy of Sciences' report *Scientific Communication and National Security* presents an attractive but incomplete solution to a political problem that contains irreconcilable social choices. It also provides an interesting example of how a "technical fix" can be used in the interactions of science and politics. The report emerged from a process in which a select group of scientists and policy-makers translated politically divisive issues into a set of cost-benefit questions based on unstated assumptions. Those questions were then substituted for the policy conflict itself and, in the process, changed the terms of the debate.

The report emerged from the discussions of a nineteen-member panel chaired by Dale Corson, President emeritus of Cornell University. Appointed by the National Academy of Sciences (NAS) in May 1982, the panel met several times during Summer 1982 with governmental officials and with representatives from various scientific and educational groups. Initially commissioned as a one-year study, the final report was prepared and published about six months after the panel was formed.

The panel was charged by the NAS

... to examine the various aspects of the application of controls to scientific communication and to suggest how to balance competing national objectives so as to best serve the general welfare.

Rosemary Chalk is an Exxon Research Fellow for 1982-83 in the Program in Science, Technology, and Society, Massachusetts Institute of Technology, and is on leave as Program Head of the Committee on Scientific Freedom and Responsibility, American Association for the Advancement of Science, Washington, DC 20005.

The original goals therefore were to identify the various social interests at stake in the scientific communication/national security debate ("to balance competing national objectives"), to formulate a set of objectives which would promote the national interest in this debate ("best serve the general welfare"), and to suggest ways in which alternative forms of information controls would promote or weaken the common good.

Political debate on these issues has centered on competing views over how U.S. national security interests should be fostered and protected: One school of thought—represented primarily by those associated with scientific and educational interests—argues that openness is an essential feature of our national strength, and that openness should be protected even though the United States might "lose control" over state-of-the-art information in selected scientific or technical fields. Those who share this concern believe that openness in science is both an end in itself—part of traditional American respect for freedom of speech—and a means to enhancing greater scientific productivity and creativity, economic growth, and education. These factors in turn not only contribute to the advancement of military strength but also independently foster a broader foundation for national security. Those who advocate controls—primarily persons with ties to the defense and/or intelligence communities—argue that without military strength there is no national security and that increased attention should be given to maintaining U.S. control over advanced technology. To foster military superiority, therefore, the Federal government should restrict (and certainly should not aid) the transfer (or "leakage") of advanced technologies or information about those technologies to adversary nations. From the perspective of the advocates of control, even though state-of-the-art

information may at times result from university research, such information should be restricted, whatever its source.

It is possible to imagine two approaches that could resolve these differing views. One approach, based on the issue of openness, could carefully review how openness either fosters or weakens national security. Asking how much openness is desirable would explore how much risk a nation should assume to maintain its open character in the face of possible losses to its military strength. Such a review would involve both a critical assessment of how concepts of national security are defined, and an examination of how competing interests between openness and military strength relate to this concept.

A second approach could be derived from the concerns of those who advocate the need for stronger controls. Rather than looking at openness as a central issue, the focus instead would be on protecting military interests, and would include analysis of threats resulting from unwanted technology transfer. Concerns about openness, or other cultural values, then become "satellite issues" ringing this central question.

From my perspective, the assignment given to the NAS panel was to seek a balance between these competing approaches. What the panel actually did, however, was to accept the latter model as the sole framework for their study, as is clear from their own re-statement of their charge:

In order to determine how and where controls might further the national welfare, it is necessary to balance many factors, including the military advantage from controls, their impact on the ability of the research process to serve military, commercial and basic cultural goals, and their effects on the education of students in science and technology. [pp. 11-12]

The central feature of the NAS study was therefore the issue of "controls" rather than openness. The panel did not attempt to develop a model based on the issue of openness. Instead it sought to derive a formula that would be responsive to the terms of the problem as presented by the defense and intelligence agencies, and yet would impose minimal damage or costs upon their own research and education interests:

[The panel sought] to develop solutions that will provide maximum benefits, both in terms of maintaining the health of the U.S. scientific en-

terprise and safeguarding national security, while incurring minimum national costs. [p. 16]

Such an approach translated the national policy debate between openness and military controls into a problem of minimizing the impact of military objectives on other national interests. The translated problem was then substituted for the policy debate itself.

From the outset, the panel looked at the question of technology transfer only in a military context. Once the members were convinced that some undesirable transfer of technical goods and information had occurred, they explored how the controls sought by the Department of Defense could be developed without seriously damaging the research and education functions of the university. In the process, the panel accepted a set of unstated premises about the military's right to dictate how national security interests should be protected in times of national conflict:

All parties have an interest in . . . research . . . and in educating . . . scientists and engineers. *These objectives must fit, however, within a system that enables the government to classify work under its sponsorship . . . and that enables the university to select only work compatible with its principal mission.* [pp. 4-5, emphasis added]

"Fitting" research and education activities into a national security context, without also addressing such activities in a context based on openness, created a major source of bias within the panel discussions. As a result, the panel did not fully explore the benefits of openness, except as a "cultural factor" that might be harmed by military controls. A notable exception to this approach is the following paragraph, which clearly identified some of the benefits:

The Panel believes that the costs of even a small advance toward government censorship in American society are high. The First Amendment's guarantee of free speech and a free press help account for the resiliency of the nation. If political authority is to be exercised effectively, there must be trust in government on the part of those affected—a trust that is promoted by openness and eroded by secrecy. Openness also makes possible the flow of information that is indispensable to the well-informed electorate essential for a healthy democracy. Openness also strengthens U.S. institutions by allowing comparison with the performance of others and nurturing adaptation to changed circumstances. [p. 50]

The panel thus succinctly identified four major benefits that result from national policies encouraging openness: national resiliency, effective political authority, a responsive democracy, and adaptation to changing circumstances. It noted that the costs of reducing these benefits are high. The report emphasized, however, that costs to military strength resulting from a policy of openness are also high.

Are these costs comparable? If so, what criteria should be used to determine which costs are acceptable? Are both costs restorable over the same time frame, or is one set of interests more vulnerable than the other? Unfortunately, the NAS panel made no effort to grapple with these questions. Instead, it chose an approach that arbitrarily placed priority on reducing damage to U.S. military interests. As a result of this bias, the report seems more concerned about the scientist who slips into areas of military concern than about military interests that may spill over into the working environment of the scientist. For example, the report noted that "scientists working at the research frontier are closer to military applications than they may have intended to be" and that some "scientists may . . . extend their research into applications of technology with military relevance." In many cases this may well be the situation, but the report nowhere acknowledged the possibility that the reverse may also be true—that is, that military concerns may be reaching beyond the technical products of scientific work into the processes of science itself: from the *what* to the *how*. Instead, the reader is left with the image of the unsuspecting scientist, poor fellow, who stumbles into areas of military application and, as a result, needs guidance.

Having translated the national security/scientific communication debate into a problem of undesirable technology transfer, the NAS panel then proceeded to develop a set of specific recommendations. First, it reviewed the extent and nature of technology transfer from the United States to the Soviet Union, drawing on briefings primarily from classified sources within the Department of Defense and the intelligence agencies. When presented with evidence of technology "leakage," the panel concluded that "there had been transfer of U.S. technology of direct military relevance to the Soviet Union from a variety of sources." They did not seek to assess how such transfer may benefit other interests, but accepted such transfer as a serious threat in itself.

The Panel then asked whether this transfer involves a significant amount of research from university sources or the open scientific literature, and concluded:

... there is a strong consensus that scientific communication, including that involving the university community, appears to have been a very small part of this transfer up to the present time. Open communication on [sic] basic research results . . . has, however, contributed to the scientific knowledge base of the Soviet Union as well as to that of other nations.

Finally, the Panel asked whether any areas of university research should be restricted because of their benefit to the Soviet Union. They concluded that "limited restrictions short of classification are appropriate" for some "narrow gray areas," and then outlined four criteria that officials should consider in deciding when to impose government controls:

The Panel recommends that no restriction of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involves a technology meeting *all* the following criteria:

- The technology is developing rapidly, and the time from basic science to application is short;
- The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;
- Transfer of the technology would give the U.S.S.R. a significant near-term military benefit; and
- The U.S. is the only source of information about the technology, or other friendly nations that could also be the source have control systems as secure as ours. [p. 5]

The panel's narrow interpretation of its task is evident in the sole emphasis on military interests.

I believe that the list would have been strengthened if the panel had added a fifth consideration requiring the military benefits of restricting sensitive information to be balanced against the costs of depriving non-military groups (e.g., the general public) of the data. This consideration would urge an assessment of the non-military value of the information deemed to be sensitive to national security concerns, and would require a true balancing of national security interests: that is, weighing a perceived military edge against factors that directly contribute to national vitality and

strength. For example, new information about the medical treatment of tropical diseases could conceivably fall within the criteria outlined by the panel. Would these criteria apply to a new development in genetic engineering which could have some application to bacterial or chemical warfare? Restricting such information in times of military conflict is at times considered to be appropriate. To do so in times of peace, however, requires stronger justification than the simple acknowledgment that the information may contribute to the military strength of an adversary nation.

The press commentaries that appeared in the wake of the NAS study were disappointingly superficial. Both major newspapers and scientific news magazines emphasized the extent to which the NAS report agreed or did not agree with the government's assessment of the need for controls. The *New York Times* (1 October 1982) reported that "there has been 'substantial and serious' leakage of American technology to the Soviet Union," but that "open scientific communications and exchanges, particularly the activities of universities, played 'a very small part' in the leakage." *Science* magazine (15 October 1982) echoed this theme, emphasizing that the NAS report validated the belief that universities were only a small part of the larger problem of unwanted technology transfer. The *Science* article reported that the NAS "failed to find evidence that leaks of technical information from universities or other research centers have damaged the national security." Neither article addressed the issue of how concerns about undesirable technology transfer had obscured the importance of questions related to the value of openness in science and in American society.

When the panel translated its charge of identifying and balancing competing national interests into a task of determining how the information controls sought by government officials could be imposed with minimal damage to university and research interests, the creation of a "gray zone" of restricted data was inevitable. Technology transfer, rather than the development of competing views over what actions best promote national security, emerged as the critical problem. As of the writing of this commentary, there has been no public assessment of the costs to national strength when the values of openness and public communication traditionally associated with American scientific work are compromised as a result of new strategic policies that place heavy reliance upon technical innovation as a primary measure of military superiority.

Given the short time-frame of the study, the temperature of the debate, and the fact that the Department of Defense was the major client for the NAS report, it may have been unrealistic to expect that the panel would seek to conduct an open-ended review of the competing interests at issue in this debate. We could have expected, however, that such studies not be framed as broad-based efforts to foster the common good when the participants accept at the outset a one-sided approach to the problem at hand without independent critique of the terms of the definition of the problem to be addressed. As a result, it is necessary to maintain a healthy skepticism toward efforts that present short-term fixes to problems rooted in historical conflicts. Choices between the strengths of an open society and the strengths of military efficiency are difficult ones to make, because they are based on competing political and social perceptions of what combination of interests best promote the common welfare. Developing criteria to assist in the resolution of these choices is a task that still remains.

733

21 JANUARY 1983 · VOL. 219 · NO. 4582

\$2.50

SCIENCE

AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE



Academic Freedom and the Classified Information System

Robert A. Rosenbaum, Morton J. Tenzer, Stephen H. Unger
William Van Alstyne, Jonathan Knight

A recent report (1) on the network of statutes and regulations which have been invoked by government officials to restrain unclassified research and travel and publication by academic researchers concluded that these restrictions abridge academic freedom significantly beyond the needs of national security. It was also argued that the nation's security is ill-served by the restrictions in that barriers to learning from others, as well as the suppression of innovative work whenever

in the Air Force who told him, a week before the symposium, that his papers had not been cleared and therefore should not be presented. The professor, while vigorously protesting, withdrew the papers.

Certain research conducted in universities may have immediate and direct national security implications. Some of that work is undertaken pursuant to Department of Defense contracts. Universities generally recognize that such ar-

Summary. Executive Order 12356, signed by President Reagan on 2 April 1982, prescribes a system for classifying information on the basis of national security concerns. The order gives unprecedented authority to government officials to intrude at will in controlling academic research that depends on federal support. As such, it poses a serious threat to academic freedom and hence to scientific advances and the national security.

its originality might be useful even to the industrial or technological progress of other nations, are necessarily discouraging to the maintenance of research leadership within the United States.

A recent event tends to justify such criticism. A university professor submitted two papers for presentation, and subsequent publication, to the 26th Annual Technical Symposium of the Society for Photo-Optical Instrumentation Engineers meeting in San Diego in August 1982. The professor's research, supported by a grant from the Air Force, was not classified, in accordance with the university's stated policy "to undertake only those research projects in which the purpose, scope, methods, and results can be fully and freely discussed." As he had done routinely in the past, the professor also sent the papers to the program offi-

rangements may compromise their commitment to academic freedom, and they vary in their policies respecting the wisdom and acceptability of such arrangements. The American Association of University Professors (AAUP) has thought it inappropriate to condemn faculties and universities for making such arrangements per se, but it has regularly expressed concern that inconsistency with respect to academic freedom is a genuine danger that all academic institutions should weigh carefully in the research and restrictions they accept.

The implication of the earlier report (1) was to favor a limited classification system, to the extent that it might minimize uncertainty and provide a less random threat to academic freedom. Ideally, a clear and circumspect classification system should state what research and pub-

lication must necessarily be treated in confidence according to needs of national security that are plain and compelling. It should enable universities and their faculties to make informed decisions about their research. Very different, and strongly objectionable, is a classification system that sweeps within it virtually anything that might conceivably be useful industrially, technically, or militarily to at least someone and that is administered by officials who feel compelled to classify as secret any information about which they have doubts.

Here we review briefly the recent changes introduced into the classification system by Executive Order 12356, issued by President Reagan on 2 April 1982. A recent report of the National Academy of Sciences Panel on Scientific Communication and National Security (2) concluded that a national policy of security through openness is much preferable to a policy of security by secrecy. We agree. We believe the enlargement of the classification system as stated in Executive Order 12356 is seriously mistaken. It poses an unwarranted threat to academic freedom and hence to scientific progress and the national security.

Summary of Recent Changes

Executive Order 12356 is the most recent presidential executive order prescribing a system for classifying and declassifying information on the basis of national security concerns. President Franklin Roosevelt issued the first such order in 1940. Succeeding executive orders were signed by Presidents Truman, Eisenhower, Nixon, and Carter. In their details, these earlier executive orders differed on such matters as what information was to be classified; for what period of time, and according to what standards. Their similarities, however, are more noteworthy than their differences. They sought to preserve the public's interest in the free circulation of knowledge by limiting classification authority, by defining precisely the purposes and limits of classification, and by providing procedures for declassification.

By contrast, Executive Order 12356 significantly broadens the authority of government agencies to classify information as secret. It removes a previous requirement for classification that damage to the national security be identifiable. It resolves doubts about the need to classify in favor of classification. It permits indefinite classification. It provides for reclassification of declassified and

This article is adapted from a report issued in October 1982 by the American Association of University Professors' Committee A on Academic Freedom and Tenure. The report was prepared by Committee A's Subcommittee on Federal Restrictions on Research. The members of the subcommittee are R. A. Rosenbaum, professor of mathematics, Wesleyan University, Middletown, Connecticut 06457; Chair, M. J. Tenzer, professor of political science, University of Connecticut, Storrs 06268; S. H. Unger, professor of computer science, Columbia University, New York 10027; W. Van Alstyne, professor of law, Duke University, Durham, North Carolina 27706; and J. Knight, associate secretary, American Association of University Professors, Washington, D.C. 20036.

publicly released information. It expands the categories of information subject to classification to include nonclassified research developed by scientific investigators outside the government.

Main Provisions

The preamble to Executive Order 12356 states that the "interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure." To prevent "unauthorized disclosure," the order establishes three levels of classification: top secret, secret, and confidential. The standards for top secret and secret are the same as in previous executive orders. However, Executive Order 12356 omits the earlier qualifying word "identifiable" in describing the damage to the national security that can justify classification at the lowest, or confidential, level. The text reads: "confidential shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security." At a congressional hearing, a Deputy Assistant Attorney General explained the deletion of the requirement of identifiability as follows:

Every new qualifier or adjective, such as "identifiable," added to the requirement of showing "damage" or any other requisite element of proper classification, raises new uncertainties or areas of ambiguity that may lead to litigation. . . . [T]he requirement of "identifiable" damage may be construed to suggest that disclosure must cause some specific or precise damage, a requirement that the government might not reasonably be able to meet in some cases. . . . Provisions of such orders should be simple, general, less complex and require no more precision than the subject matter reasonably allows. The requirement of "identifiable" damage fails on all these counts.

In the event that a government official is uncertain about the security risk of some information, the doubt will be resolved in favor of classification pending a final determination within 30 days. In addition, if there is doubt about the level of classification, the information will be classified at a higher level, also pending a final decision within 30 days. Once the information is classified, it can remain so at the discretion of government officials "as long as required by national security considerations." There is no provision in Executive Order 12356 for justifying the need for classification beyond a stated period of time. (President Nixon's executive order called for automatic declassi-

fication after 30 years, unless it was determined that continued classification was still necessary and a time for eventual declassification was set; President Carter's executive order established a 5-year declassification period.) The latest order makes no comment on whether declassifying information is generally desirable.

If information is declassified, it may be reclassified under Executive Order 12356 following the requirements for classification. Information that has been properly declassified and is in the public domain apparently may remain "under the control" of the government (the order defines information as "any information or materials . . . that is owned by, produced by or for, or is under the control of the United States Government") and thus can be reclaimed by the government.

The executive order provides for limitations on classification. It states that "basic scientific research information not clearly related to the national security may not be classified." Early drafts of the order had not included this provision; it first appeared in the executive order issued by President Carter. It was retained mainly as a result of protests from the scientific community. However, it is not clear what this provision actually safeguards.

Sanctions for violations of the executive order may be imposed on the government's "contractors, licensees, and grantees."

Comments

National security obviously requires some classification of information as secret. It is also obvious that freedom to engage in academic research and to publish the results is essential to advance knowledge and to sustain our democratic society.

The possibility for friction between classification and academic freedom is always there. The friction can be reduced if classification is invoked before research has begun and is cautiously applied for a limited period of time and only to matters of direct military significance. Classification defeats its own purpose, however, if it imperils the freedoms it is meant to protect. In our judgment, Executive Order 12356 does exactly that. It gives unprecedented authority to government officials to intrude at will in controlling academic research that depends on federal support. It allows classification to be imposed at whatever stage a re-

search project has reached and to be maintained for as long as government officials deem prudent. Academic research not born classified may, under this order, die classified.

The provision in the executive order that "basic scientific research information not clearly related to the national security may not be classified" carries the suggestion that it may be classified if it is determined by the government to be "clearly related to the national security." This standard for classification is looser still than "could be expected to cause damage to the national security." We may be reading too much into this provision; we hope that it will be interpreted as an exemption and nothing more. Unfortunately, even with its most favorable gloss it is a weak safeguard for scientific inquiry. The government official who cannot fix a clear relationship between scientific research and national security but nonetheless has doubts could still classify government funded or contracted research consistent with other provisions in the executive order.

In the pursuit of knowledge, academic researchers should not have to look backward either in hope of favor or in fear of disfavor. In an era of reduced federal support for research except in the area of national security, and with investments in research programs and facilities significantly reliant on previously allocated federal funds, academic researchers are under great pressure to submit to classification no matter how restrictive or apparently arbitrary the demand. The adverse effects on academic freedom and thus on the advancement of knowledge and on the national security can be grave.

The executive order can inhibit academic researchers from making long-term intellectual investments in research projects that are potentially classifiable. It can serve to foster unnecessary duplication of research efforts. It is likely to inhibit the sharing of research methods and results with professional colleagues, because something that a government official can call harmful to the national security might unwittingly be revealed. Classification, or the worry that it might be imposed, could result in the isolation of academic researchers, cut off from the free exchange of ideas and exposure to constructive criticism. Those concerned in government with the uses of new knowledge are not likely to obtain the benefit of the widest possible evaluation of their plans and projects. All of these consequences of the executive order are likely to be felt outside as well as within

the field of research in which classification is imposed.

The government has not put forward any compelling reasons for instituting a system of classification that is so at odds with previous systems. The government's own reports, including reports issued by the Department of Defense, seriously question the cost, effectiveness, and need for more classification. They draw particular attention to the dangers of overclassification.

Executive Order 12356 requires drastic revision in order to be tolerable to a

community of scholars committed to free inquiry. The application of the order to nonclassified information, which is already subject to potential restraints under existing laws and regulations, is at best superfluous. The heavy emphasis on classification is misplaced: the provision for reclassification should be removed and the standards for classification rewritten so that they do not sweep unnecessarily broadly and thereby significantly threaten academic freedom.

If the government's executive order or its successor continues to deny due rec-

ognition to the need of the independent research scholar for academic freedom, the cost will be borne not only by the researchers who are affected but by the nation as a whole.

References and Notes

1. R. A. Rosenbaum, M. J. Teazer, S. H. Unger, W. Van Alstyne, J. Knight, "Federal restrictions on research: Academic freedom and national security," *Academe: Bull. Am. Assoc. Univ. Prof.* 68, 17a (September-October 1982).
2. National Academy of Sciences, *Scientific Communication and National Security* (Washington, D.C., 1982), vols. 1 and 2.
3. The present address of S. J. Unger is Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, N.Y. 10598.

Japanese Industrial Development and Policies for Science and Technology

Toshio Shishido

In this article I describe Japan's industrial development and Japanese policies for science and technology. In the process of industrialization and modernization, Japan imported many new technologies in a wide variety of fields and at the same time made great efforts to improve

which lasted from the mid-1800's until the end of the 19th century, the metal, chemical, and machine industries became increasingly dependent on imports (Fig. 1). The technological development of these industries, and of the light industries that produced such important ex-

Summary. Two important factors that contributed to Japan's economic success were government investment in industrial development and the early recognition that a good educational system is a prerequisite to technological progress. Government policies promoted the importation of technologies from Europe and North America and encouraged the education of students abroad. This facilitated the rapid development of Japanese industry and the adaptation of foreign technologies to local conditions. Many of the methods used to develop industry in Japan could be used to advantage in developing countries today.

these technologies and adapt them to local conditions. The success of these efforts depended on many factors, the most important of which were the education of the general population and government initiative and support.

The development of industry in Japan over the last 100 years can be divided into four stages. During the first stage,

The author was formerly vice president of Nikko Research Center, Tokyo, Japan, and is now vice president of the International University of Japan, Mito-ku, Tokyo 106. This article is adapted from a paper prepared for the International Development Council of Japan.

port items as textiles, was therefore limited until the beginning of the second stage in about 1900. The third stage of development began after World War II, when Japan had to undergo a rapid development process to catch up with the advanced technology of the West. By the early 1970's the level of technology in Japan had surpassed that in Europe and reached about the same level as in the United States. Now, in the fourth stage of development, Japan's attention is turning from imitative to creative technology.

Stage 1. Policies for Promoting Industries

The Meiji government (1868 to 1912) recognized that increased production and the promotion of industries were essential for establishing a solid economic foundation for the construction of a modern state. The immediate target of its policies was the curtailment of imports and the promotion of exports, with greater emphasis on the former. With the opening of the country to foreign trade, foreign products poured into the domestic market, putting pressure on the domestic cotton-yarn industry as well as other industries, and causing a chronic deficit in the international balance of payments.

To counter this trend, the introduction of modern industry was urgently called for. However, there was little private capital available, so that nothing short of direct investment by the government could accomplish the desired objectives. Since the government aimed at encouraging the private sector to follow its example, it made direct investments covering the operations of its own factories, the construction of railways, the exploitation of mines, and the management of experimental stations.

The Ministry of Engineering, created in 1870, was charged with the responsibility for encouraging the development of many industries and running the mines, railways, and communications. During the ensuing 15 years it operated the government-owned factories and mines, many of them expropriated from the former Tokugawa Shogunate and the feudal lords. Tomioka Spinning, for instance, was established in 1872 by the government; it was equipped with French-made spinning machines and was operated by French techniques.

In this manner, the Meiji government

NATIONAL SECURITY AND SCIENTIFIC COMMUNICATION

A summary of responses received in reply to
a letter from the AAAS Committee on Scientific
Freedom and Responsibility

June 1982

Committee on Scientific Freedom and Responsibility
American Association for the Advancement of Science
1515 Massachusetts Avenue, N.W.
Washington, D.C. 20005

EXECUTIVE SUMMARYIntroduction

In March 1982, the Chairman of the AAAS Committee on Scientific Freedom and Responsibility (Leonard Rieser, Provost, Dartmouth College) wrote to 100 leading American scientists and engineers on the topic of science and secrecy. The purpose of Dr. Rieser's letter was to gather responses from a selected sample of scientists in universities and industry, and from scientists who served as government advisers, to the following questions:

- Is there a basic conflict between the principle of open scientific communication and national security?
- Is the current system for classifying or restricting access to scientific and technical information on national security grounds too restrictive, generally satisfactory, or too permissive?
- How should scientists and engineers respond to government efforts to restrict or classify the communication of research information on the basis of national security interests?

The individual responses to these questions included replies from presidents or top corporate officials of IBM, Westinghouse, General Electric, General Motors, and Lockheed; from the presidents of Harvard University, University of Washington, University of Pennsylvania, Stanford University and UCLA; from seven American Nobel Laureates; from the presidents of engineering and scientific societies affiliated with AAAS and from the chairpersons of several AAAS sections.

The responses provide a broad range of opinion in reply to Dr. Rieser's questions. No attempt has been made to categorize the replies. Instead, the contents of the letters are being used to inform interested persons of the nature and scope of concerns of an important group of American intellectual and business leadership. It is hoped that these views will stimulate further thought and discussion of the complex issues involved.

This summary provides a brief overview of the opinions and concerns expressed in the letters received by the AAAS Committee on Scientific Freedom and Responsibility. It is intended to stimulate further discussion of the important issues to be addressed in developing government controls over scientific communication on the basis of national security concerns. A more detailed report describing highlights from each letter is available from the Committee office.

Is There A Basic Conflict?

Replies to the first question posed in Dr. Rieser's letter were focused primarily upon the principles involved in the current debate about national security controls on sensitive scientific or technical information. Several respondents indicated that there was an inherent conflict between the principles supporting unrestricted communication in science and the concerns for secrecy in the interest of national security.

Most of the replies noted that open scientific communication and national security concerns complemented each other in that both supported scientific progress as a basic objective. However, the respondents noted that there may be conflicts over the best means to achieve this objective. A few selected statements illustrate this range of opinion:

The conflict between the requirements of national security and the free exchange of information among members of the science and engineering communities is perennial and unavoidable. (President William P. Gerberding, University of Washington)

There is, in my opinion, no "basic" conflict between the principle of open scientific communication and national security. To sacrifice the former in pursuit of the latter would be counterproductive, serving neither the security nor the scientific interests of this nation. This is not to say that in a particular instance the two values might not collide, but such instances are overshadowed by the tradition of general compatibility. (President C. Peter Magrath, University of Minnesota)

I believe there is a basic conflict between the principle of open scientific communication and our national security. Both are extremely important, and we must be very careful that as we attempt to resolve conflicts we do not excessively compromise either. (Thomas G. Pownall, President, Martin Marietta Corporation)

A general conclusion that can be drawn from a review of the letters is that the respondents hold both concerns--open scientific communication and national security -- as twin objectives, although they differ substantially in defining the best means of achieving these goals and the priority which they would assign to each objective.

"Vagueness" of the Controls

The second question posed in Dr. Rieser's letter asked the respondents to comment on the current system for classifying or restricting access to scientific and technical information. An area of strong concern which surfaced in the replies focuses on the issue of "vagueness" of the current and proposed restrictions, as well as the "unevenness" of their application. Some examples:

Although there is undoubtedly a conflict between open communication and national security in certain specialized areas, I do not believe that this can be generalized to conclude that there is a basic conflict between the principle of open scientific communication and our national security. One of the major difficulties identified during the present debate is the vagueness associated with prescribing the areas to be regulated. Without a clear focus on the problem being addressed, there is a tendency to regulate this area much too broadly. (Vice-Chancellor Albert A. Barber, UCLA)

(My faculty is) concerned with what is seen as a growing tendency on the part of Government to haphazardly interfere with currently satisfactory policies concerning the free and open exchange of unclassified scientific information. Most agreed that if changes are perceived to be necessary, clear regulations should be adopted which explicitly outline the limitations to be imposed. (President Sheldon Hackney, University of Pennsylvania)

My associates and I feel that the greatest problem that exists with our policy is its uneven application. This uneven application not only permits truly important compromise of important technology but it also inordinately frustrates those investigators who in good conscience conform to the rules. In my view, it is important that we find a way to make our present system enforceable. (President R.A. Fuhrman, Lockheed Missiles & Space Company, Inc.)

The Current System is About Right, But ...

The respondents differed in their attitudes towards the current system of classifying and restricting access to sensitive information. (Ed. note: the "current" system was that in place in March 1982, prior to the new Executive Order on classification). Several persons thought that the current controls were about right, while others saw them as too lax or too rigid:

The current system (of classification) is restricted to work performed directly by and for the DOD or DOE.... My experience suggests that the current system is administered in a generally satisfactory fashion. It is ponderous, expensive and inconvenient. (Vice President George F. Mechlin, Westinghouse Electric Corporation)

The current system as it has been administered in the last several years is probably about right -- that is not too restrictive or too permissive. Generally government classifications are not abused and are used to a minimum. Our experiences in applying for export control licenses through the Department of Commerce have generally been good and have not imposed undue restrictions or delays. (Executive Vice President, William C. Hittinger, RCA)

A few replies indicated that the authors saw the current system as being too permissive:

I believe we have become too permissive in allowing research information to be freely communicated which compromises our national security. We should establish a policy which assures that research information of significant importance to national security is appropriately restricted. (President Thomas G. Pownall, Martin Marietta Corporation)

Several other scientists saw the current system as too rigid, and indicated that classification controls are more often used to cover up waste and inefficiency than to protect information which, if disclosed, could damage national security interests:

It is a demonstrable fact that security classification and secrecy impedes scientific and technical progress very effectively, as can be clearly seen when comparing the Russian scientific achievement with our own, or, in more local experience, in comparing the performance of "open" laboratories like Bell Labs with other industrial organizations or DOD laboratories. Secrecy tends to cloak inefficiency, ignorance, and corruption more often than it hides genuine technical secrets. (P.W. Anderson, Nobel Laureate, Bell Laboratories)

What Information Should/Should Not be Controlled

The authors were encouraged to give examples of information which they believed should or should not be controlled on the basis of national security concerns. Their examples follow:

The most difficult aspect of public policy regarding this "dual use" technical know-how relates to the international interchange of information within the academic sector. IBM's experience in long range fundamental research strongly supports the conclusion that openness and freedom from excessive government regulation are essential requirements for reasonably paced progress and for effective diffusion to applications. (Vice President and Chief Scientist Lewis Branscomb, IBM)

The difficulty with regulations is that they are not self-adaptive, and require doing the impossible: defining the essence of the importance of undefined knowledge and unmade inventions. The essence of creative activity is that the most important thing is the least expected, and by definition, that which is not encompassed in the prior knowledge or art, and thus not in the prior regulation. (Vice President Robert Frosch, General Motors and President of the American Association of Engineering Societies)

The very nature of "basic research" is such that the probability of any given piece of information having value to an enemy is very low. Further, the time it takes to apply such information is very long -- often more than a decade -- which makes it very nearly impossible to safeguard. Between these two factors I think it doesn't make sense to classify or restrict basic research information. Executive Vice President William Hittinger, RCA)

In principle, a schedule of automatic declassification by stages is quite effective. In reality, the system falters at times, as in the case of the shuttle Columbia. Access to research done on Dinosaur, a similar shuttle project of the 1960s, would have precluded some reworking of old problems. The information, despite urging from those working on the project, was not declassified in time to be of any use. (President William Gerberding, University of Washington)

One simply cannot justify restricting information which might -- however remotely -- play a role in the further protection, maintenance or restoration of human health regardless of political, geographical, economic or any other boundaries. (Associate Vice Chancellor Karl J. Hittelman, University of California, San Francisco)

The current system of classification and restricted access to scientific information has not entered into my own sphere of investigations and research. I am concerned, however, that a rigid paranoid approach to classification could conceivably assign a restricted, non-accessible classification to many types of data I deal with, such as energy resources reserve calculations as well as production capabilities. (Director Arthur A. Socolow, Pennsylvania Bureau of Topographic and Geologic Survey and Chair AAAS Section on Geology and Geography)

It is quite possible that discoveries made in an open environment might have sufficient military impact that these discoveries should be classified and their open dissemination restricted.... Examples of cases where unclassified research might develop items of a classified nature are: 1) Discovery in routine chemical investigations of new toxic agents which might be used against us; 2) uncovering of new chemical reactions which might be used in high energy laser reactions; 3) development of semiconductor processes which make ICBM sensing substantially more easy; or 4) accidental coming across techniques for high-strength metals which could substantially change tank armor capabilities. (President R.A. Fuhrman, Lockheed Missiles and Space Company, Inc.)

Are Regulations the Answer?

Two areas of concern emerged in the responses to the third question posed in Dr. Rieser's letter. When asked how scientists and engineers should respond to government restrictions on sensitive technical information, some authors indicated that the individuals who generate the information themselves should serve as the keystone in developing controls over the dissemination of the information. Others indicated that more formal regulations should guide individuals in deciding how to disseminate sensitive information:

It behooves scientists to take the initiative in assuming responsibilities, as individuals. Awareness of the problem and discreet actions to protect information vital to national security can be more effective than rules and regulations by government agencies. In instances where their scientific research leads to results with potential for military applications, scientists should exercise appropriate restraint in the dissemination of their findings. Only in this way can we hope to avert onerous measures on the part of government that would be harmful not only to science but to the national interest as well. (Paul Flory, Nobel Laureate, Stanford University)

Scientists and engineers should be concerned about achieving an effective balance between open communication and national security to protect our national interest and principles, and I believe they are so motivated. However, I cannot accept the view that individual scientists and engineers are best equipped to be the sole judge if their work is critical to national security. (Vice President A. Thomas Young, Martin Marietta Aerospace)

A second area of concern emerged in these responses as well: how to maintain progress in American research and development activities. A few examples follow:

There is much talk about the "hemorrhaging of technology" to other nations as a result of the traditional policy of openness. What's needed is a counter-balancing analysis with suitable documentation of the crucial importance to the health of the American scientific and technological enterprise of our policy of openness in information exchange. All my interactions with industrial research leaders, as well as my own experience lead me to conclude that this openness is, indeed, one of our great advantages. The harmful effects of its loss or restriction would have to be weighed before any form of official review of the research is ever adopted as being in our national interest. (Sidney Drell, Deputy Director, Stanford Linear Accelerator Center)

My real concern is that the U.S. R&D establishment continue to operate so as to produce the results that maintain technology leadership. Two requirements of this are a reasonable degree of free and open communication among U.S. scientists and engineers and ready access to foreign generated technology. I do fear that the currently proposed, dramatic broadening in the International Traffic in Arms Regulations to include large fields of technology so broadly defined as to include most of the nonmilitary work in laboratories such as ours will seriously inhibit the conduct of R&D. Some proposals would require State Department review for almost everything we do prior to publication, presentations where foreigners might be present,

and many interactions with U.S. universities with foreign professors or students in attendance. Clearly, such a broad-gauge censorship would be counterproductive and highly detrimental; a compromise must be found that will protect the really vital military interests without imposing such deleterious controls. (Vice President Roland W. Schmitt, General Electric)

An approach to the problem which attempts a legalistic and regulatory definition of classified and unclassified subjects, and is essentially procedural in its approach, is going to fail. It will fail not only because it is divisive, but because it will set up forces in the research system which will be destructive.... The essence of the social situation that I would like to see constructed, in analogy to the ones that have succeeded in the past, is one in which the research community interested in a subject area and the government community interested in its development and use consider themselves all to be parts of the same community of interest; interested in the research for its own sake, and interested in its development for national purposes. (Vice President Robert Frosch, General Motors)

Long-Term Consequences

A few respondents offered some general comments regarding possible consequences resulting from more restrictive controls on scientific and technical information, particularly if such restrictions are applied to academic research work:

Unless scientists take seriously the problems pertaining to the subject of your letter, the current system for classifying and restricting access to scientific and technical information is likely to be extended further into areas that are peripheral to national security. Consequences of moves in this direction should be evident to everyone engaged in scientific research. Some of the current research in universities would be driven from university laboratories to the "underground" of external institutes and facilities. This is clearly a prospect that not only would be abhorrent to faculty, but one that would be detrimental to the advancement of important branches of science and technology as well. (Paul Flory, Nobel Laureate, Stanford University)

If universities were to withdraw from restricted work, federal agencies could attempt to carry on the research in their own facilities. But this policy would force the government to run the risk of severely retarding progress by proceeding without the help of a large proportion of the leading scientists in the fields involved.... Even if universities could be persuaded to continue the research under government restrictions, the costs could easily outweigh any benefits to national security. Many able scientists might turn to other fields rather than submit to the controls. (President Derek Bok, Harvard University)

Conclusions

The above comments reflect a wide range of concerns among a sample of representatives of the American scientific and engineering leadership. Although there is presently no unanimity or consensus around a single position, the various perspectives presented in the letters are still in a very early state of formulation. The balancing of interests which support national security objectives with concerns about the importance of maintaining open scientific communication procedures remains an ill-structured problem.

However, the responses do indicate that the individuals who replied to this poll believe that the questions posed are important ones. The responses also indicate that the academic and corporate officials contacted through this poll feel strongly about the need to foster more dialogue with the officials who are developing our government's national security policies. There was general support for more structured interaction among the governmental, industrial and academic sectors in order to narrow the points of agreement and disagreement in this controversy.

The goal of the AAAS Committee in initiating this project was to stimulate and provoke a broader public discussion of the competing interests at issue in the development of policies which seek to limit the communication of sensitive scientific and technical information. The Committee urges that professional and government groups seek additional ways to broaden the opportunities for scientists, engineers, and policy-makers to educate themselves on the important issues involved in this controversy. The Committee also urges these groups to make their concerns publicly known in the policy-making process and to sponsor public discussions of the key issues in order to stimulate new ideas and possible remedies to the problems posed in these letters.

AAAS Committee on Scientific Freedom and Responsibility

Leonard Rieser (Chairman)
Dartmouth College

David Bazelon
U.S. Court of Appeals

Kenneth E. Boulding
University of Colorado

Thomas Eisner
Cornell University

Esther Hopkins
Polaroid Corporation

Arnost Kleinzeller
University of Pennsylvania

Dorothy Nelkin
Cornell University

Warren Niederhauser
Rohm and Haas Company

Elena O. Nightingale
Institute of Medicine

Herman Pollack
George Washington University

Harold Relyea
Library of Congress

Stephen Unger
Columbia University

Victor F. Weisskopf
Massachusetts Institute of Technology

Anna Harrison (AAAS President-Elect)
Mount Holyoke College

CSFR Program Head
Rosemary Chalk, AAAS

HIGHLIGHTS

Letters were received from the following persons:

A. University Officials

- Albert A. Barber (Vice Chancellor-Research Programs, UCLA)
- ✓ Derek C. Bok (President, Harvard University)
- William P. Gerberding (President, University of Washington)
- Sheldon Hackney (President, University of Pennsylvania)
- Karl J. Hittelman (Associate Vice Chancellor, Academic Affairs,
UC-San Francisco)
- C. Peter Magrath (President, University of Minnesota)
- Robert M. O'Neil (President, University of Wisconsin)
- Robert M. Rosenweig (Vice President for Public Affairs, Stanford University)
(with enclosure prepared by Donald Kennedy,
President, Stanford University)
- ✓ Michael I. Sovern (President, Columbia University)

B. Corporate Officials

- Lewis M. Branscomb (Vice President and Chief Scientist, IBM)
- Robert A. Frosch (Vice President, General Motors Corporation)
- George H. Heilmeyer (Vice President, Corporate Research, Development and
Engineering, Texas Instruments)
- W.C. Hittinger (Executive Vice President, RCA)
- George F. Mechlin (Vice President, Research & Development, Westinghouse
Electric Corporation)
- Thomas G. Pownall (President, Martin Marietta Corporation)
- Roland W. Schmitt (Vice President, Corporate Research and Development,
General Electric)
- Morris Tanenbaum (Executive Vice President, AT&T)

C. U.S. Nobel Laureates

- P.W. Anderson (Bell Laboratories)
- N. Bloembergen (Division of Applied Sciences, Harvard University)
- Paul J. Flory (Department of Chemistry, Stanford University)
- Roald Hoffman (Department of Chemistry, Cornell University)
- David H. Hubel (Department of Neurobiology, Harvard Medical School)
- Arno Penzias (Vice President, Research, Bell Laboratories)
- Roger W. Sperry (Division of Biology, California Institute of Technology)

D. AAAS Affiliate Presidents and Section Chairs

- Marilyn C. Bracken (Chair, AAAS Section T - Information, Computing and Communication and Associate Assistant Administrator for Toxics Integration, Environmental Protection Agency)
- Felix E. Browder (Chair, AAAS Section A - Mathematics and Chairman, Department of Mathematics at the University of Chicago)
- Peter J. Denning (President, Association for Computing Machinery)
- Robert B. Gaither (President, American Society for Mechanical Engineers)
- Charles G. Overberger (Chair, AAAS Section C - Chemistry and Vice-President for Research at the University of Michigan)
- Arthur A. Socolow (Chair, AAAS Section E - Geology and Geography and State Geologist and Director, Pennsylvania Bureau of Topographic and Geologic Survey)
- Helen M. Tepperman (Chair, AAAS Section N - Medical Sciences and Professor of Pharmacology at SUNY-Syracuse College of Medicine)
- Stuart A. Umpleby (President, American Society for Cybernetics)

E. Members of the Defense Science Board and DOD Advisers

- Sidney D. Drell (Professor and Deputy Director, Stanford Linear Accelerator Center)
- R.A. Fuhrman (President, Lockheed Missiles & Space Company, Inc.)
- A. Thomas Young (Vice President, Research and Engineering, Martin Marietta Aerospace)

Restrictions on Academic Research and the National InterestTable of Contents

- 1 - Introduction
- 2 - Policy Changes Bearing on Publication and Scientific Exchange
- 3 - Issues in the Current Debate
- 4 - The Openness of University Research
- 5 - Controls on Research and the Dissemination of Information
 - Problems of Implementation
 - Control by Classification
 - Control by Restricting Publication
 - Control by Distinguishing between Basic and Applied Research
 - Control by Restricting Collegial Communication with Foreign Nationals
 - Control by Restricting Access of Foreign Students and Postdoctorals
- 6 - Conclusions and Recommendations

W. D. Cooke, Vice President for Research
Cornell University, Chairperson

Thomas Eisner, Section of Neurobiology and
Behavior

Thomas Everhart, Dean, College of Engineering

Franklin A. Long, Program on Science, Technology
and Society

Dorothy Nelkin, Program on Science, Technology
and Society

Benjamin Widom, Department of Chemistry

Edward Wolf, Director, National Research and
Resource Facility for Submicron
Structures

Introduction

This paper was prepared at the request of the Panel on Scientific Communication and National Security which is under the sponsorship of the National Academy of Sciences. The authors were charged with presenting an assessment of the impact that more rigorous controls on the free flow of information in the academic community would have on the nation's universities and on the national research effort.

In the preparation of this analysis advice and comment was solicited from a number of sources. A draft was distributed to the members of the Committee on Export Controls of the DOD-University Forum and was discussed with them. Copies were also sent to a number of universities and a cross section of Cornell faculty for review. Subsequent drafts were revised in the light of the comments received. To ascertain current policies, information was solicited from twelve major research universities. The responses received were reasonably uniform and in agreement with the basic positions presented in this document. Even so, the views expressed in this document are those of the authors alone.

Our analysis covers two rather different but related topics: controls on the dissemination and publication of the results of research produced by U.S. scientists and engineers; and restriction on their interaction with foreign nationals, including foreign students in U.S. universities.

It is not our intention to weigh the disadvantages of controls on research results against the problem of flow of scientific and technical information to foreign countries. With incomplete access to the full significance of this flow and its effect on national security, we confine our discussion to the adverse effect of increased control of research and communications on the university's teaching and research functions, and the resulting negative impact on the nation's programs in these areas. It will be the responsibility of the Panel which can more fully evaluate the adverse effect of openness in university teaching and research on national security, the fraction of the actual technology flow attributable to university programs, and the potential effectiveness of controls to weigh these conflicting factors in their recommendations.

The extent of the impact of the new restrictions on university research and teaching programs which are described in this report will depend on the breadth of coverage of scientific fields and how the regulations are interpreted. Depending on this outcome, the analysis can be applied either to specific areas of research or more broadly across universities.

Policy Changes Bearing on Publication and Scientific Exchange

Constraints on the publication and dissemination (written or oral) of work with evident military significance have existed for years. However, these concerns have recently been extended and reinterpreted on a new assumption - that the tradition of open communication in science and technology increasingly conflicts with national security needs. This assumption is explicitly expressed in several recent documents. In September 1980, the Department of Defense issued a brochure stating that scientific exchanges and communication practices were enhancing Soviet military power and that open scientific literature was adverse to military security interests. The brochure questioned the wisdom of various scientific and technological exchange programs, arguing that they were often not really reciprocal. Other recent government documents emphasize the need to "protect our scientific communities" against Soviet acquisition of science and technology. These concerns are reflected in a number of actual or proposed policy changes. Those bearing on university teaching and research are as follows:

Under the Invention Secrecy Act, patentable discoveries can be placed under "secrecy orders" if disclosure is deemed detrimental to national security. This has mainly been enforced in the case of inventions developed by people working in defense agencies or under defense contracts, but it has recently been more broadly applied.

The government can control and restrict the export of technical information under the International Traffic in Arms Regulations (ITAR) deriving from the Arms Export Control Act of 1976. Administered by the Department of State, these regulations cover the export of technical data, defined to include unclassified information useful in the design of "any technology which advances the state-of-the-art or establishes a new art in any area of significant military applicability." Under this law the government can require that scientific papers be approved by a cognizant agency prior to publication.

- 3 -

In addition, the Export Administration Act regulates export of goods and services not controlled by ITAR. This is administered by the Department of Commerce, but the Defense Department plays an active role. In principle, the Act covers conferences, lectures and meetings and requires the Secretary of Commerce to examine the export of all technical data including the 1.5 million scientific and technical articles that appear annually in the open literature and which are available for foreign perusal.

Several incidents in 1980 clearly reflect the trend towards increasingly comprehensive interpretation of these secrecy laws through restrictions on scientific exchange. The Department of Energy issued an order requiring government clearance of any communication between DOE contractors and Soviet scientists. The Commerce Department forced the American Vacuum Society to withdraw its invitation to Soviet bloc scientists to attend a conference on magnetic bubble memory devices, asserting that oral exchanges of information with foreign nationals fall under Export Administration Regulations and that sponsors would have to obtain an export license before admitting communist-bloc scientists. Then, the State Department refused to issue visas to eight Soviet scientists who had planned to attend a conference on laser and electro-optical systems.

State Department officials have also contacted universities requesting that certain departments planning to accept foreign students submit detailed information on what they would be learning, who they would be working with, and where they planned to travel. The intention is to follow the movements of individual foreign students and through the host university control their access to information.

Another critical new development, from the point of view of our current concerns, is the extension of the Export Administration Regulations to cover ideas as well as hardware; "Information of any kind that can be used or adapted for use..." "Oral exchanges of information" are included as a form of export. The most comprehensive legislative proposal has been to extend the provisions of the Arms Export Control Act. This Act currently requires a license from the State Department in order to export "critical technology." The proposed extension of the Act introduced to the House of Representatives in 1982, redefines the class of transactions subject to licensing requirement to include unclassified data and ideas that might pertain to military technology. It requires that scientists who want to publish research or even

- 4 -

to exchange notes and drafts in certain areas, or to speak overseas on any subject relating to a technology listed in the United States Munitions List, obtain a prior license from the Secretary of Defense in consultation with the Secretary of State and the Secretary of Energy. The scope of restricted subjects could include all research related to computers, laser and cryptography, but the list and its limits are far from clear. In 1981, the DOD extended the list of restricted subjects on its "Militarily Critical Technologies List" to include 620 technologies. The list itself is published but the interpretive details that would provide guidance to universities is classified.

Finally, Executive Order 12356 has greatly increased government powers to classify research even in areas not clearly related to national security. All government grantees are personally responsible to comply with classification constraints if they have any reason to believe their work has security implications. The Executive Order drops the crucial requirement previously established: that classification requires evidence of "identifiable damage, and that decisions imposing secrecy must be balanced against the public's right to know." To cover contingencies, the Order mandates that: "If there is reasonable doubt about the need to classify information...the information shall be considered classified."

Issues in the Current Debate

Recent initiatives, threatening to impose sharply increased controls on academic research and education, have generated a debate of substantial proportions as evidenced by an outpouring of papers, speeches, letters to the editor and editorials. The Department of Defense maintains that the present openness of university research harms the security of the nation and therefore requires the imposition of some form of control over the flow of information. On the other hand, the university community maintains that a) controls on the dissemination of ideas and developments in research would have a detrimental effect on the research enterprise in the United States and unless clearly and directly related to important military applications would not be in the national interest; b) because of the coupling of research and advanced training activities in U.S. universities, such controls will also impede our capacity to train new scientists, attract high quality people to do research in these areas, and thus to maintain the very strengths we are trying to preserve. Both sides in the debate support their position in the genuine

belief that the interest of the nation is better served by the course of action they espouse.

The University community maintains that the generally open nature of American universities is one of the primary reasons for the strength of U.S. science and technology compared to other nations. The overwhelming practice among university scientists is one of free discussion and prompt publication. The university community believes that this characteristic openness, encouraging cross fertilization, enhancement of ideas, criticism of conclusions, and verification of findings is an important aspect of a strong national research capability and an essential factor in the education of future scientists. If research carrying restrictive covenants were to become a major component of university research efforts, it would be impossible to carry out the universities' educational mission and difficult to attract faculty and students to these areas. Given the position of universities in the overall national research effort, this would be detrimental to the national interest.

The Openness of University Research

The practices of universities emphasize open communication on campus. Therefore, the policies of most universities exclude classified research on campus and allow limited delays in publication but reject censorship of publications by sponsors. Although individual faculty members or groups of faculty might occasionally be willing to accept certain restrictions, such acceptance would be excluded by general university policies. These policies are applied evenhandedly to all sponsors, governmental and non-governmental.

The notion that university based research is an open activity does not mean that all the research ideas in the mind of a faculty member must be freely shared with anyone. Situations can exist where some faculty members decline to discuss ongoing research results with others. For example, if an exciting new area has been discovered, a researcher may delay full dissemination of initial information in order to refine the results or even to capitalize on advance knowledge for subsequent research options or patent protection. In these cases, however, students would have full access to all developments

including the capacity to incorporate materials into theses that will become public documents. Researchers tolerate such delays in the release of information on the assumption that the individual deserves some limited advantage from a successful discovery. However, prolonged secrecy would expose an individual to sanctions from colleagues. Academics present or publish their research as quickly as possible, consistent with retaining some advantage in future research efforts.

Despite the above comments, it must be acknowledged that the declining time lag between basic research and its commercial application may set in motion a set of incentives for faculty researchers that encourage proprietary rather than open behavior in their research activities. The thrust toward commercialization, e.g., biotechnology, led some researchers to treat new research results and materials as proprietary so that they, or companies in which they have an equity position, can capitalize on possible financial developments. While such situations occur, they are currently rare and hardly condoned. Proprietary behavior in science is simply felt to be unacceptable. University administrators, concerned with conflicts of interest, are developing policies to address these problems.

Despite aberrations, the tradition and practice of university researchers remains one of open and free communication and prompt publication.

Controls on Research and the Dissemination of Information

Problems of Implementation

Implementing the proposed constraint on communication of technical information presents enormous problems when compared to the export of tangible devices. The restrictions, both proposed and in force, are cumbersome and vague. The inclusiveness of the provision of the Executive Order on classification are themselves classified. Similarly, the definition of "strategic information" in the Arms Export Control regulations provides few guidelines for implementation. When applied to the export of concepts or ideas, such ill-defined regulations are unenforceable except in an arbitrary and capricious manner. Restrictions on foreign nationals are vague. They call for "minimal involvement" in research - a limit that is pragmatically difficult to define. Restrictions suggest exceptions for basic research; again posing practical problems of implementation in the context of contemporary research.

The vagueness of regulations leaves the burden of proof on the individual researchers who want to lecture or publish, or otherwise disseminate their work. Researchers themselves must decide if their work is subject to export laws. Under the Arms Export Control Act, they must show that dissemination would not damage national security and, conversely, that withholding information would be contrary to the national interest. And they must exercise this responsibility without adequate information. This vagueness is characteristic of the proposed control mechanisms.

The following sections attempt to analyze these control mechanisms - their effects, and the problems of implementation in the university context.

Control by Classification

The most stringent level of research control is formal federal classification. While most secure, the utility of classification must be weighed against its negative impact on overall national objectives.

The policies of most major universities prohibit classified research on campus and, in the present situation, few universities would be willing to change this policy. Hence, classification would exclude involvement of universities in areas of research which were classified. Not only would the expertise of many of the most talented university faculty members in important research areas be lost, but also the education of new scientists and engineers with advanced research training would be curtailed. If the areas of classified research are significantly broadened, these losses of talented students and faculty would be counterproductive to national goals.

Some universities accept classified research in off-campus facilities. As a rule however, regular faculty members are only peripherally involved in such facilities, usually in a consulting mode and students may have even less interaction. In these arrangements, the primary role of the university is the management of the facility, and the research staff is little different than those found in an industrial or government laboratory. Since these laboratories can engage faculty consultants, in most cases there appears to be little difference between an off-campus classified research facility and an industrial or government laboratory. Control over publication within these facilities is common as are restrictions on visits by foreign nationals. But these restrictions would not be relevant to normal university research and teaching.

Control by Restricting Publication

Current university policies generally preclude the acceptance of research contracts which do not give the principal investigator final authority over publication. The right of the researcher to decide what material is to be published is consistent with the traditions of an open academic community and society and results in a more effective research effort.

One of the factors that attracts scientists to university faculties is the opportunity to select their research areas, interact freely with other scholars, and to publish their findings. Restricting this opportunity would exacerbate the present difficulty in recruiting - at university pay scales - new faculty members, particularly in certain areas (e.g., engineering). Junior faculty depend on a tested publication record for promotion and graduate students require the promulgation of their research findings as part of the requirements for their degrees. In the evaluation of students and postdoctorals for faculty and other positions, published research accomplishments play an essential role. Considering the importance attached to publication, the vulnerability of only a small percentage of manuscripts submitted for clearance would discourage many academic scientists and students from participation in research covered by such arrangements.

While university policies prohibit contracts requiring a sponsor's approval of publications, they often permit contractors to review manuscripts prior to publication. Such provisions are designed to allow industrial sponsors a prior review to protect intellectual property rights and patent possibilities. These procedures are applicable to all sponsors including federal agencies. If such a system were adopted as a control mechanism for some areas of research, it is important that time limits be established for such reviews to avoid extended publication delays.

The contractual right to review manuscripts may be different in the case of federal sponsors than for other sponsors. In effect, with a federal agency, the author would be seeking an advisory legal opinion as to the publishability of the material. If the agency decided that publication would be illegal, barring compromise, the only recourse an author would have would be the courts.

Another possible arrangement for the control of publications involves a voluntary submission of articles for review prior to publication. This procedure, adopted by some cryptologists, may not be easily adaptable across a broader area of science and technology. First, most cryptology research is directly related to national security whereas research in other areas is less directly related. Secondly, in cryptology a single agency with significant expertise, indeed a small group within the agency, is responsible for the review. If applied more broadly, reviews would be undertaken by different offices varying greatly in expertise and capacity leading to inconsistent and uninformed reviews. Finally, in cryptology the volume of work and the number of researchers is small. These conditions are not present in most other areas. Thus, problems are foreseen in the administration of any procedure involving reviews whether they be voluntary or contractual.

The control of the dissemination of information at the point of publication is an inefficient method of retaining confidentiality. Publication is the final step in a continuing process of information transfer. Discussions occur among students and faculty across research groups. Departmental seminars are usually the first formal step in the dissemination of research results. Information is also transferred from researchers in one institution to colleagues working in the same area in other universities. In the latter stages of the research, presentations are made at national meetings. Thus, by the time the material is published, the results are already known to a broad spectrum of individuals. Unless foreign citizens are excluded from the universities and from national meetings, some transfer of research results to foreign countries is inevitable even without publication. To decide at the time of publication that the information is too sensitive to be in the public domain, overlooks the fact that the most significant aspects of the research may have already been promulgated orally or by distribution of pre-publication information.

Control by Distinguishing between Applied and Basic Research

Various attempts have been put forward to differentiate basic from applied research as a criterion for the exportation of technical information. The distinction between basic and applied research is a difficult one. Attempts to neatly distinguish the two areas has a long history but seem to be increasingly difficult. The issue has arisen again in the current context in an effort to focus control in the applied research area. The attempts to

- 10 -

make this distinction do not imply that applied research is necessarily sensitive or that it should not be done in universities.

At the two extremes of these general research classifications such distinctions are possible. For example, the recipe for building a nuclear device can be distinguished from the discovery of endogenous morphine-like substances (endorphins) in the brain of man; the first clearly applied research with probable reason for security control classification; the second basic research with no reason for control.

However, if the consideration moves to mission-oriented research and, in particular, if the mission-oriented research has dual (or multiple) end-use, then the problem of such distinctions becomes blurred. For example, laser ranging studies of the moon provide a direct test of the equivalence principle in Einstein's theory of relativity, but they also generate more accurate information on certain geodetic parameters that affect the precision of Air Force weapon systems.⁽¹⁾ Do we classify the laser ranging data and the laser range finder and thereby "protect" the data useful to the Air Force weapons system, and exclude the test of the theory of relativity?

The present controversy on export control of technical information has focused on the use of technology of semiconductor microelectronics (and the ubiquitous computer) in both military and consumer electronics. The control of information in this field is the antithesis of the openness responsible for the rapid growth and economic vitality of the semiconductor microelectronics market and could hamper the competitiveness of American industry in this sector.

The hardware and software engineering data that go into the production of specific weapons systems can be controlled, but the specific concern that most universities now face with respect to their microelectronics research is the control of generic research and engineering topics, for example, electron beam lithography, reactive ion etching, and molecular beam epitaxy. Excessive restriction of the applied research and development in subset disciplines of the microelectronics industry would close down most university microelectronics centers in the United States. This is not a desirable result either for

(1) This example was taken from a list of current basic research projects in "Basic Research in the Mission Orientated Agencies" Report of the National Science Board, National Science Foundation 1978. Page XVII.

- 11 -

government or for universities, nor is it consistent with the government's desire to have universities participate in the VHSIC program.

Most engineering schools in the United States carry out research and instruction in this gray area of mission-oriented, dual-use research with varying mixes of identifiable basic and applied research. The reported percentage of each varies according to the nature of the evaluation. In two separate recent NSF publications, the Federal Government alternately reported \$3.5 billion ⁽¹⁾ and \$2.75 billion ⁽²⁾ in basic research support in 1977. The discrepancy of \$800 million, over 20%, arose in large part from the different definitions of basic research which are difficult to reconcile unambiguously.

If clear-cut categorization is required, the distinction between basic and applied is not a workable guideline for the export control of technical information and data. The unavoidable difficulties of such a classification arises from the fact that research is a continuum of investigative endeavors ranging from efforts to produce new fundamental knowledge to producing new manufacturing "recipes" ⁽³⁾ for new products. University research and development spans this entire range.

An example from microelectronics might be helpful. The sequence of specific procedures that lead to the manufacture of integrated circuits, often called "recipes" is the type of information that most United States semiconductor companies hold as "company private or secret" and should be under export control. Often these recipes have more than 150 specific steps for the completion of a particular type of semiconductor integrated circuit.

Progress in integrated circuit manufacture most often occurs by small evolutionary changes in the process recipe, but sometimes by revolutionary changes that replace major steps in the processing; for example, ion implantation replacement of thermal dopant diffusion and electron beam lithography replacement of photolithography for mask fabrication.

-
- (1) National Patterns of R&D Resources, Funds, and Manpower in the United States, 1953-1977, NSF 77-310, p. 4 as referenced in (1) on p. 10
 - (2) Federal Funds for Research, Development and Other Scientific Activities, Vol. XXVI, NSF 77-317, p. 49, as referenced in (1) on p. 10
 - (3) The term "recipe" has been used previously in the revisions to the EAR and in the Report of the DOD Science Board Task Force on VHSIC

Research on generic topics related to semiconductor processing, such as ion implantation, electron beam lithography and reactive ion etching, produces new knowledge that can be applied to new or modified recipes, but in itself does not constitute technical data or information that is susceptible to export controls. This is because each generic topic is only one small input to a very large sequence of process steps, each of which has to be specially adapted by extensive engineering development before it becomes part of the manufacturing "recipe." Furthermore, most technologically advanced countries are carrying out such research and it is being reported in the open technical journal literature.

Controls on publication or dissemination of information on ion range versus energy (ion implantation) plasma chemistry (reactive ion etching) and radiation chemistry of polymers (electron beam lithography) would remove universities from their leadership role in this research. Furthermore, because industry has found university research to be useful, as evidenced by the recent creation of the Semiconductor Research Cooperative to support university research, export controls on generic topics of semiconductor science and technology would slow and might terminate our country's leadership position in semiconductor microelectronics.

Restriction or control of university research in discreet parts of subsets of the "recipe" technology should be carefully distinguished from the use of advanced recipes to fabricate state of the art integrated circuits. Most universities do not have state of the art manufacturing facilities or recipes and therefore do not constitute a channel for high technology leakage to adversary nations.

Control by Restricting Collegial Communication with Foreign Nationals

One method of partially controlling the transfer of scientific information outside of the U.S. is to restrict the access of foreign nationals, both in the U.S. and abroad, to communication and the publication of research results.

The imposition of additional restrictions on foreign nationals must be weighed against the potential loss of the contributions of foreign science and scientists to the U.S. effort, and the practicality of developing an efficient system to control access.

One factor which must be considered is the international character of science. International cooperation and collaboration in basic research is widespread in the research community. Scientific and technical journals are distributed worldwide. International meetings are frequent. Scholars, including those in science and engineering, are peripatetic as witness the travel plans of the annual list of U.S. recipients of Guggenheim fellowships, or the facts that three quarters of the world's scientific literature is published in journals of countries other than the author's own, and 16% of all science and technology articles are co-authored by individuals from organizations in different countries. (1)

Another contribution of foreign science to the overall national and international scientific effort is indicated in the world's scientific literature. In 1979, the U.S. proportion of the world's scientific articles was 21% in chemistry, 30% in physics, and 41% in engineering and technology. (2)

The mobility of scientists on an international scale has benefited the U.S. The contribution of foreign scientists to the American effort can be illustrated by the award of Nobel Prizes. Since 1950, of the prizes in physics awarded to Americans, 33% of the recipients were foreign born. The percentages for chemistry and medicine are 17% and 38% respectively. Two-thirds of these scientists received their advanced education in other countries.

The essential point is that there is a true international community of scientists. It exists because of the considerable mutual benefits in international information exchange and collaboration. Any effort to exclude U.S. scientists and engineers from this international collaboration would meet with widespread resentment. It is doubtful if it could succeed. It is even more doubtful whether success would be to the net benefit of the U.S. Developments by foreign scientists and scholars have been, and will continue to be, of great importance to U.S. programs. As an example, details on the USSR-developed Tokomak machine for studying nuclear fusion were first presented in the U.S. at a physics seminar at Cornell University, and since then Tokomak has become the focus of the major U.S. effort in this field.

(1) Science Indicators 1980, National Science Board 1981. The author's country is determined by the author's organization and the journal's country is defined as the country where it is published.

(2) Science Indicators 1980, National Science Board 1981. p. 17, 47

Control by Restricting Access of Foreign Students and Postdoctorals

One of the more obvious contributions to U.S. science by foreign nationals is their role as students and postdoctorals in university research. About half of the doctorates in engineering are foreign nationals. ⁽¹⁾ as are 70% of the postdoctorals ⁽²⁾ and their role is increasing. In the period 1976 to 1979, the number of U.S. full-time graduate students in science and engineering declined slightly while the number of foreign nationals increased 29%. ⁽³⁾ The contribution of these young scientists to the university research mission is noted by the statement, "In these two fields (chemistry and engineering) many departments would find it difficult, if not impossible, to maintain research productivity without participation of foreign postdoctorals." ⁽²⁾

After completion of their studies in the U.S. some of these young scientists return to their own countries and, in many cases, play an important ambassadorial role. Others remain in this country and increase our technological competitiveness. Unfortunately, information has not been found on the percentage of foreign scientists remaining in the U.S. labor force or on university faculties. However, some indication of the extent to which these foreign scientists flow into the U.S. effort can be deduced from the following information: for doctorates in engineering 28%, and in physical sciences 29% have immigrant status; for those engineers with definite plans, 53% plan on employment in the U.S., and 15% plan further study (the equivalent figures for the physical sciences are 47% and 19% respectively; ⁽⁴⁾ for postdoctorals in engineering, 33% have immigrant status; ⁽⁵⁾ for all engineering postdoctorals, 30% plan to take positions on university faculties in the U.S., and 30% plan to work for U.S. industry. ⁽²⁾ From this information it appears that a substantial number of foreign students and postdoctorals take up residence in this country

- (1) Summary Report 1980. Doctorate Recipients from United States Universities. national Research Council 1981
- (2) A Report of the Committee on the Study of Postdoctorals in Science and Engineering in the United States. National Research Council 1981
- (3) Foreign Participation in U.S. Science and Engineering Higher Education and Labor Markets. NSF 1981
- (4) Foreign Participation in U.S. Science and Engineering Higher Education and Labor Markets. NSF 1981, p. 45
- (5) A Report of the Committee on the Status of of Postdoctorals in Science and Engineering in the United States. National Research Council 1981, pgs.384,395

- 15 -

Despite the importance of foreign students, implementing security restrictions by excluding foreign students from discussions or by controlling access to university seminars would result in the withdrawal of most universities from those areas of science which would be affected. Nor would universities be willing to accept a monitoring and control function over foreign visitors.

Regulations which would exclude foreign students from certain research projects within an academic department raises insurmountable problems. There is considerable interaction among university research groups and they are frequently housed in the same laboratory space. In any healthy academic department there is constant intellectual exchange and wide discussion of research results among its students and faculty. This is a highly desirable educational process and it is unlikely that such information exchange could be curtailed except by formal classification. Thus, it would ordinarily not be possible to pursue a research project which is subject to controls on the transfer of information to foreign nationals in a department having foreign students.

There seems to be no viable solution to the problem. The use of visa controls as a means of selective by excluding students is not feasible because most entering students have little information about their future thesis topics. To eliminate the problem by the total exclusion of foreign students is hardly acceptable considering their importance to the research effort.

Finally, to refuse all research projects which are covered by ITAR and EAR is hardly a desirable solution. The actual impact of such a decision on university research would depend on the breadth of coverage of the regulations and how they are implemented.

- 16 -

Conclusions and Recommendations

There is undoubtedly a significant transfer of American science and technology to the Soviet military operation. The more advanced countries routinely transfer their technology to other nations through normal international trade. In addition, illegal transactions and clandestine operations provide information to bolster the military and commercial potency of other nations. Inevitably, those countries which produce the highest quality research contribute more research knowledge to other countries than they receive in return. And for those nations that are both preeminent in science and technology and place a high value on democratic traditions, the problem of technology export can be severe. While efforts should be made to reduce that flow of science and technology that directly affects our national security, it should be recognized that the amount of critical information transferred directly from universities is relatively limited. According to Admiral B. R. Inman, Deputy Director of Central Intelligence, "only a small percentage comes from direct technical exchanges conducted by scientists and students." (1)

Whatever level of increased restrictions on university programs is deemed necessary for national security, the methods used to control the transfer of identified technologies should be consistent with the actual demonstrated magnitude of the problem. They also should recognize that such action could serve to undermine the contributions that universities have made in maintaining our current scientific and technological preeminence. It is in this spirit that we make the following recommendations:

- 1 - The experience of World War II demonstrated that universities were willing to set aside their traditional openness and to virtually abandon their educational effort in the face of clear and present danger to the security of the nation. In the current situation, a case has not been made to the broad academic community which would convince them of the necessity for controls.

(1) Testimony, May 11, 1982. Senate Governmental Affairs Committee Permanent Subcommittee on Investigations

- 17 -

Therefore, it is recommended that the proposed controls over university research and the arguments for imposing them be disseminated to the academic community.

- 2 - Most faculty members are totally confused as to their responsibilities under the export control regulations. It is not known if the regulations are limited to a few narrow areas, or apply broadly across university research. Hence, they do not know if their research is covered by the regulations and what they should do if it is. It is imperative that existing regulations be clarified. We believe that such clarification will illustrate the limits on implementation.

It is recommended that a group such as the Export Controls Committee of the DOD-University Forum, after consultation with appropriate federal agencies, disseminate information on the export controls regulations and develop guidelines for faculty members concerning problems that may arise.

- 3 - America is fortunate in having a close and cooperative relationship between its government and its academic community. This has served the nation well. To preserve this productive relationship,

It is recommended that careful consideration be given to the actual procedures adopted. Rules and procedures should be no more onerous than fully justified and, to enhance their effectiveness, they should reflect an understanding of the importance of free communication to university programs, and thus to the entire national research effort as well as our capacity to train advanced scientists and engineers. Whatever controls are placed on academic researchers, it is important that they be reasonable and understandable so as to be persuasive to the academic community.

- 4 - Some of the uncertainty and confusion surrounding export controls could be reduced if conditions were incorporated in requests for proposals and research contracts. This would allow universities and individual faculty members to choose whether to accept the contractual conditions or forego the research support. In establishing contractual

- 18 -

conditions, it should be realized that most universities are unwilling to accept classified projects on campus. Nor are they willing to accept arrangements that involve limitations on discussions with students or require controlled access to seminars. Many universities also reject contracts which require approval of publication. However, arrangements which require a prior review of manuscripts are often acceptable.

Given the present confusion in the implementation of export controls,

It is recommended that when controls are deemed to be necessary that they be clearly specified by the federal agencies in the terms of all such individual contracts for university research.

It is realized that such a procedure would not exempt individuals from the control regulations. However, a mechanism of prior evaluation would go far in decreasing uncertainties.

- The impact of export controls on university research depends on just how broad and inclusive the areas to be covered will be. Scientific research in universities is at the frontier of existing knowledge and conceivably a great deal of it could ultimately have military application. If widely implemented across broad areas of science, the regulations could have a serious effect on federally sponsored research programs by making it virtually impossible for universities to accept the support. Given the importance of university research to the scientific and technological leadership of the nation and the difficulty in distinguishing between applied and basic research,

It is recommended that when controls must be imposed that they be limited to clearly defined areas of significant danger to national security. The recommended guidelines for controls should be based solely on whether the information deals with specific procedures or recipes to produce an article of military importance to national security.

- 19 -

- 6 - Senior foreign visitors make a substantial contribution to university research efforts through the exchange of knowledge.

It is recommended that restrictions on foreign visitors be kept to a minimum. Visa restrictions by the Department of State should be imposed judiciously with sensitivity to the free functioning of our academic institutions and only in subject areas where it can be shown that significant harm will occur if they are not imposed. It should not be expected that universities would exert a control and surveillance role over foreign visitors.

- 7 - Foreign graduate students in the U.S. present a special problem since their specific research is unknown when they arrive. Given that it is impossible to control the movement of students and discussions among them in an open campus environment,

It is recommended that the control lists be reviewed and restraint be exercised in applying the ITAR and EAR to university research. Interpretation should take into consideration the value of foreign students to the research effort of the nation and the open communication that is so vital in an academic setting.

Scientific Freedom, National Security, and the First Amendment

James R. Ferguson

It is now apparent that the American scientific community is approaching a critical point in its relations with the federal government. Until recently, the conduct of most scientific work in this country proceeded on a well-founded assumption: that it would remain free from official intrusion or state regulation (1). Since 1979, however, the federal

view is the belief that the American military must depend on the technological superiority of its weapons systems to offset the quantitative superiority of the Soviet Union (6, 7). The critics charge that restraints on scientific expression are both ineffectual as a means of curbing the transfer of technology and inconsistent with the requirements of scien-

Summary The Supreme Court may soon be asked to decide an important issue of First Amendment law arising from the government's efforts to restrict the dissemination of "militarily critical" technological knowledge. To resolve the issue, the Court will first determine whether technological knowledge qualifies for a full measure of protection under the free-speech clause of the First Amendment. The Court will then address the government's stated justification for restricting the contested information. This inquiry will evaluate both the gravity of the asserted danger to national security and the likelihood of its occurrence

government has frequently acted in the name of national security to impose restraints on important aspects of the scientific endeavor. Most notably, in an effort to curb the export of "militarily useful" technologies, the Administration has applied the existing set of export controls to domestic scientific symposiums, university research programs, and even the presentation of scientific papers (2, pp. 97-107; 3-5).

This effort to restrict the dissemination of applied scientific knowledge has sparked heated debate. The government maintains that the normal avenues of scientific communication often contribute to a "technology leakage" that enhances the military capabilities of the Soviet Union (6, 7). What underlies this

scientific progress (2, pp. 42-45; 4, 8). In this view, America's technological supremacy is due in large part to policies that promote the free circulation of scientific and technological information.

The debate has thus far addressed the government's effort to control the export of applied scientific knowledge as a broad question of public policy. It seems likely, however, that the major issues in the controversy will soon be tested under narrower, legal principles in a court of law. If so, the government will almost certainly rely on one of two congressional statutes as authority for its restraints on the transmission of technological knowledge.

One of the statutes is the Arms Export Control Act (9), which empowers the

State Department to license the export of all military articles listed in the International Traffic in Arms Regulations (10). As defined by those regulations, the relevant articles consist not only of war-making devices such as aircraft and explosives but also of "any information" used in the production of military arms (10, sect. 125.01). Equally important, the regulations broadly construe the term "export" to include the noncommercial transmission of information in domestic settings such as scientific symposiums (10, sect. 125.03; 11).

The other statute is the Export Administration Act of 1979 (12), which differs from the arms regulations in two respects. First, it authorizes the Commerce Department to license the export of "dual use" technologies that are subject to both military and civilian applications. Second, it deals principally with the export of technologies to "controlled countries" such as the Soviet Union, Poland, and East Germany. Like the arms regulations, however, the Export Administration Act restricts the domestic release of any information used in the production of commodities having a military value (13). Furthermore—and again like the arms regulations—the Export Administration Act imposes stiff criminal penalties on those who willfully violate its licensing requirements (12, sect. 2410).

In these statutes Congress has provided considerable authority for governmental restraints on the export of "militarily useful" technologies. This fact alone, however, will not end the legal inquiry in cases where the government has invoked the statutes to restrict the open, domestic communication of applied scientific knowledge. On the contrary, in such a case, a major issue will arise concerning the validity of the legislation under the free-speech clause of the First Amendment.

To resolve this type of issue, the Supreme Court has consistently relied on a well-defined analytical framework designed to determine whether the state's interest in regulation is sufficiently im-

The author is a visiting scholar in law and science at Yale Law School, New Haven, Connecticut 06520.

portant to justify an abridgment of First Amendment freedoms. In the rest of this article, I will examine the ways in which the Court's mode of analysis can accommodate the difficult First Amendment issues arising from the imposition of restraints on the open, domestic communication of technological knowledge (14).

First Amendment Fundamentals

Like other guarantees in the Bill of Rights, the free-speech clause of the First Amendment stakes out a zone of individual freedom by identifying a specific activity to be protected against unwarranted governmental intrusion. The enforcement of such guarantees is left to the Supreme Court, the branch of government removed from public accountability and vested with the power to invalidate official acts that encroach on the protected freedoms. This power of judicial review, however, carries the risk that the Court will frustrate the democratic process by freely substituting its own preferences for the enacted will of the public's elected representatives. Accordingly, under prevailing constitutional theory, the Court's power is properly exercised only when its decisions are rigorously based on principles derived from the text of the Constitution (15, 16).

These larger considerations have often guided the Court in deciding cases arising under the free-speech clause of the First Amendment. Rejecting the notion that all speech is absolutely immune from official regulation, the Court has determined the degree of protection to be accorded to various categories of expression by looking to the major values that underlie the free-speech guarantee. These values, according to the Court, can be summarized in three propositions. First, the right of free speech advances the citizen's interest in self-fulfillment by enabling him to realize his full potential through the free expression of opinions, beliefs, and ideas. Second, the guarantee of free speech serves an important social function by promoting the widest possible circulation of socially useful information. Finally, the right of free speech is essential to a democratic form of government, for it ensures that all information bearing on various policy issues is fully disseminated to the public (17, 18).

Though the Court has not yet adjudicated the issue, it seems clear that scientific communications contribute to each of these interests and thus warrant as much protection as political tracts, literary works, or any other variety of

speech. Indeed, a system of free scientific expression not only enables scientists to draw on the work of colleagues but also tests the validity of hypotheses against current data and opposing views. In these ways, it promotes the discovery of scientific truth and fosters the intellectual advances that contribute to the collective wisdom (2, pp. 42-45; 19, 20).

In the case of purely technical data, however, more difficult questions arise. For example, does technical information having only military uses warrant the same degree of constitutional protection as political speech or basic scientific knowledge? In all likelihood the Court will answer in the negative, for it has previously held that analogous "lesser" forms of expression do not stand on the same constitutional footing as more traditional varieties of speech. For example, the Court has held that commercial advertising occupies a "subordinate position in the scale of First Amendment values" and thus warrants only a "limited measure" of constitutional protection (21; 22, pp. 651-656).

Most forms of technological knowledge, however, are subject to a wide range of uses, some of which have military value but most of which contribute directly to the material welfare of the community. This point is clearly illustrated by many of the "militarily critical" technologies that have been cited by the Department of Defense—for example, laser technology, semiconductors, computer hardware, and infrared technology (23). Given the obvious social value of such technological achievements, the Supreme Court will probably hold that the broad category of technological knowledge warrants a full measure of constitutional protection, while noting an exception for information that is subject only to military applications (19).

Once this larger question is decided, the Court will not assess the social value of the technical data at issue in a given challenge to a governmental restraint. Rather, it will simply note that the information in question falls within the category of fully protected speech and will then turn its attention to the government's countervailing interest in regulation. At this point, a crucial issue will arise: given the strong constitutional presumption in favor of free speech, just what burden of proof must the state carry to justify its imposition of restraints on the information? Or, to put it in legalistic terms, what standard of review will the Court apply to the government's stated justification for the challenged restrictions?

Determining the Standard of Review

To determine the relevant standard of review, the Court will focus on two broad questions. First, does the government have a possessory interest in the underlying information? If so, the Court will apply a mere "reasonableness" standard to any governmental restraints imposed on government employees in an effort to preserve the secrecy of the data. Thus, for example, in *Snepp v. United States*, a recent case involving a book published by a former CIA agent, the Court broadly upheld the state's power to impose "reasonable restrictions" on the dissemination of governmental information obtained by government employees (24). In addition, the Court pointedly noted that this general principle applies "even in the absence of an express agreement" between the government and the employee (25, p. 303).

In like manner, the Court will probably sustain any reasonable restraints imposed on the dissemination of information resulting from the government-funded research of private parties. Indeed, in such a case, the government's restraints will likely be upheld on either of two grounds: (i) the state, by financing the underlying research, acquires a property interest in the resulting information or (ii) the researcher, by accepting the public financing, agrees to restrictions that might otherwise be constitutionally impermissible (19, 26).

On the other hand, if the state attempts to regulate the dissemination of nongovernmental information by private parties, the Court will apply a far more demanding standard of review. In such a case, the weight of the state's burden will be determined by a second line of judicial inquiry focusing on the precise way in which the government has restricted the free-speech right.

On this issue, there are two major possibilities: either the state has imposed a "subsequent punishment"—usually in the form of criminal penalties—on individuals who have already published the restricted information, or it has blocked the dissemination of the data by issuing a "prior restraint." In the case of a subsequent punishment, the Court will uphold the action only if the state can demonstrate a "compelling" interest in regulation (22, p. 602; 27)—a burden of proof that stands as the modern analog of the well-known "clear and present danger" test formulated by Oliver Wendell Holmes (28). In the case of a prior restraint, the Court will apply an even more demanding standard of review, since the government is seeking to block

the timely dissemination of information and ideas. Indeed, on the evidence of the so-called *Pentagon Papers* decision (*New York Times v. United States*) the Court will uphold the restraint only if the government can show that a "grave" and "irreparable" harm will almost surely result from publication of the data in question (29).

Clearly, under either standard of review the state is faced with an exceedingly difficult task. Nevertheless, the Court has indicated that in some "exceptional" cases, principally in the area of national security, the government's interest in regulation may be sufficient to warrant a direct infringement on fully protected speech (29). The remaining question, therefore, is: Just how will the Court assess the importance of the state's concerns to determine whether they are adequate to justify an abridgment of First Amendment freedoms?

Weighting the State's Interest in Regulation

The Court has held that the strength of the government's interest in regulation is determined in large part by two independent factors: the nature of the harm that the state is seeking to avert and the likelihood of its occurrence (30, p. 843). In particular, the crucial inquiry centers on whether the "gravity of the evil," discounted by its improbability, justifies such invasion of the free speech right as is necessary to avoid the danger" (31). With this approach, the seriousness of the threatened danger will affect to some extent the showing required of the government on the "likelihood of occurrence."

The Court has long recognized that "no governmental interest is more compelling than the security of the Nation" and that this interest sometimes requires the state to protect the secrecy of certain kinds of information (24). On the facts of a given case, however, the state could not rely on the mere assertion of a national security threat, for the Court will make its own inquiry into the nature and magnitude of the harm said to result from publication of the data at issue (30, p. 843).

The state's argument on this score will undoubtedly stress the unique nature of technical knowledge and, in particular, the unique way in which this variety of speech can harm the public. Under classic First Amendment theory, most forms of human communication contribute to the larger social exchange of opinions, beliefs, and ideas and do not threaten in

any way the material welfare of the society. Indeed, on this theory, the speech of an individual generally cannot cause any harm to the community except by influencing others to adopt an erroneous or misguided position. The theory further holds that the government has no genuine interest in suppressing a "dangerous" idea, since the alleged error or fallacy can be exposed through an additional exchange of views (22, pp. 605-606; 32).

These general considerations, however, do not always apply to technological knowledge, which often gives rise to dangers of a more immediate and tangible kind. In particular, technical know-how, although rarely contributing to the general exposition of ideas, often confers the power to alter the material conditions of life in important new ways, some of which may prove harmful (19, 30, 33). For example, in the case of new technologies having military applications, the underlying know-how can provide a hostile nation with the capability of committing harmful acts it would not otherwise be able to commit.

This point was clearly underscored by the decision of a federal district judge in *United States v. The Progressive* (34). In that case, the government asked the judge to enjoin a magazine from publishing an article outlining the design of a hydrogen bomb. In granting the injunction, the judge stressed that the case differed in important ways from the *Pentagon Papers* case, which dealt with a classified history of the Vietnam War (29). Most notably, according to the judge, the case before him concerned "information dealing with the most destructive weapon in the history of mankind, information of sufficient destructive potential to nullify the right to free speech and to endanger the right to life itself" (34). Thus convinced that publication "could pave the way for thermonuclear annihilation of us all," the judge found that the government had met its heavy burden of justifying a prior restraint (34, 35).

In the case of nonnuclear technologies, the government has also invoked the name of national security to limit the dissemination of technical information having possible military applications. For example, at a recent international symposium on optical engineering, the Department of Defense blocked the presentation of a large number of unclassified papers on topics ranging from microelectronics to infrared technology (2, pp. 106-107; 36). In so doing, the department underscored its concern that advanced work in "critical" technologies

could aid a foreign adversary in the development of more effective weapons systems (36). The National Security Agency has recently monitored the efforts of research cryptographers to develop undecipherable computer communication codes (2, pp. 120-125). According to agency officials, the free publication of this work could threaten the inviolability of codes used by the American military or provide a hostile power with an impenetrable communication system (2, p. 123; 7).

In the light of these examples, it is useful to rank the various types of national security information according to the nature and magnitude of the dangers posed by the resulting capability. This effort applies, however, only to those cases in which the government has first demonstrated two important points: (i) that the information at issue is indeed subject to the asserted dangerous use and (ii) that the information is not currently available to the receiving nation from another source (19).

Assuming these facts can be established, the most serious danger would arise from technical capabilities that could alter in major ways the current balance of international military power. This category would include technologies that directly conferred on the Soviet Union a new offensive capability or an effective countermeasure to American weapons systems. It would also include technologies that exposed the United States to new threats by providing a smaller adversary with a destructive power that it had not possessed before.

These are examples of "sudden and disastrous giveaways" (37). There are other capabilities that, if acquired by a hostile nation, could result in a number of lesser harms to the nation's security. Most significant is the wide range of militarily useful technologies that could enable a foreign adversary to add incrementally to its current military strength by (i) directly improving the performance of its weapons systems, (ii) enhancing its communications network, or (iii) increasing its knowledge of American military capabilities (38). Examples of such technologies are electrooptical sensors, solid rocket propulsion systems, satellite technology, navigation and guidance subsystems, microprocessors, and microelectronics (2, pp. 18-20; 6, pp. 5-15).

A less immediate harm would result from technologies that enabled a foreign adversary to improve its military research and development. The most significant are technologies associated with the use of the computer for correlating

experimental data with theoretical models (39). Other well-defined technical methodologies are used to "guarantee reliability, explore the limits of design, and reveal new phenomena that can affect the next generation of weapons" (39).

A slightly different harm to national security would result from technologies that enabled a foreign power to upgrade its manufacturing capability in industries of military importance. For example, microelectronics and computer technologies are important in the development of in-flight guidance systems (6, p. 13), while precision ball bearings are important in the production of missiles and other military hardware (6, p. 7).

Finally, it is possible that the export of some technical capabilities could undermine foreign policy goals that are closely linked to the nation's security. The export of some types of technical knowledge, for instance, might undermine a trade embargo designed to influence the international behavior of the Soviet Union.

Turning to the question of the likelihood of occurrence, the Court will address the probability that a third party will use the information at issue to develop the new capability. This line of inquiry will consider both the complexity of the technology and the skills of the receiving nation. The need for the inquiry arises in part from the fact that the impersonal transmission of technical knowledge is rarely an effective method of transferring technology (38; 40, p. 29). As a general rule, the normal channels of intellectual communication convey only the broad outlines of technical design and theory (40, pp. 67-73). What is usually not published or codified is the body of associated know-how that constitutes the art of the technology (40, p. 73), typically including methods of operation, organization, and manufacturing procedures. This is particularly true of emerging technologies with few previous applications (40, pp. 73-74).

Accordingly, the Court's inquiry into the likelihood of occurrence will focus on the ability of the receiving nation to absorb the knowledge at issue and put it to use. For example, if the receiving nation has a high level of technical expertise in the relevant area, the government could show with virtual certainty that that nation will put the information to an immediate military use. If the receiving nation lacks any of the needed skills or resources, the state could show only a possibility that the knowledge will be put to a significant use in the foreseeable future.

Together with the gravity of the threatened harm to national security, the Court's finding on the likelihood of occurrence will generally determine whether the state's interest in regulation is sufficient to warrant the restriction of First Amendment rights. Assume, for instance, that the government can show that the Soviets have sufficient skills to acquire a new military capability by exploiting an American breakthrough in directed energy weaponry. On these facts, the Court will no doubt agree that the government's concerns are sufficiently compelling to warrant an abridgment of First Amendment freedoms. This will probably hold true, moreover, even if the government concedes that the Soviets will eventually acquire the capability anyway, since the maintenance of a military lead time can be highly advantageous (41). On the other hand, if the threatened harm to the nation's security is less serious, the state's case will be correspondingly weakened, and all the more so if the receiving nation is shown to lack the requisite skills or resources to absorb the technology.

Less Restrictive Alternatives

The crux of conventional First Amendment analysis lies in the Court's effort to determine whether the restricted information gives rise to a substantial danger and thus warrants governmental regulation. However, if this issue is resolved in the state's favor, the Court will pursue a further line of inquiry focusing on the government's regulatory technique. In particular, the Court will determine whether the restraints on speech imposed by the state are more extensive than necessary to serve its underlying concerns (42). Accordingly, even if the government can demonstrate a "compelling" interest in regulation, the Court will invalidate the challenged restraints if it finds that a "less restrictive alternative" could serve the asserted interest equally well.

A useful illustration of this principle is offered by *Central Hudson v. Public Service Commission of New York* (43). In that case, the Public Service Commission of the state of New York issued an order prohibiting all public utilities from promoting the use of electricity. The commission reasoned that such a ban would decrease the demand for electricity and thus further the state's interest in the conservation of energy resources. The Supreme Court agreed that this interest was sufficient to warrant some restriction of commercial speech but

found that the state's blanket prohibition was more extensive than necessary to further that interest. The Court noted, for example, that the commission's order prevented utilities from promoting electrical services that would reduce energy consumption by diverting demand from less efficient sources. On this ground, therefore, the Court found that the commission's order was unconstitutional.

This type of inquiry might well become relevant if recent proposals to alter the export control statutes are passed into law. For example, under one such proposal (44), the Arms Export Control Act would be amended to cover communications of any kind—technical or otherwise—dealing with any of a broad range of restricted technologies (4). This type of regulation, however, would clearly be more extensive than necessary to safeguard the nation's security, since many communications dealing with the restricted technologies have no military value. Consequently, any regulatory scheme based on this proposal would be subject to a stern First Amendment challenge on the grounds that there are less restrictive alternatives.

Conclusion

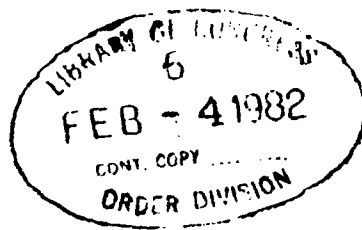
What is most striking about the Court's method of First Amendment adjudication is that it takes into account virtually all the commonsense perceptions that have informed the general policy debate on the government's effort to control the export of scientific and technical knowledge. Indeed, if the Court applies its standard analysis to this issue, it will not only give due weight to the value of scientific freedom but will also examine critically the nature and magnitude of the threatened harm to national security. In addition, it will address a variety of other considerations, such as the technical skills of the receiving nation and the reasonableness of the regulatory technique. By incorporating each of these factors into a method of adjudication that formally allocates the burden of proof, the Court's approach provides a well-defined analytical framework for accommodating the claims of scientific freedom with the legitimate interests of national security.

References and Notes

1. The one notable exception to this general rule is research that is sponsored and classified by the government—for example, the Manhattan Project.
2. National Academy of Sciences, *Scientific Communication and National Security* (Washington, D.C., 1982), pp. 97-105.
3. *U.S. Keshava, Science* 215, 635 (1982).

4. S. H. Ungert, *Technol. Rev.* 85 (No. 2), 30 (1982).
5. Committee on Operations, *The Government's Classification of Private Ideas*, H.R. Rept. No. 96-1540, 96th Cong., 2d Sess. (1980).
6. Central Intelligence Agency, *Soviet Acquisition of Western Technology* (Washington, D.C., April 1982).
7. B. Inman, "National security and technical information," paper presented at the AAAS annual meeting, Washington, D.C., 7 January 1982, F. Carlucci, *Science* 215, 140 (1982); U.S. Department of Defense, *Soviet Military Power* (Washington, D.C., 1981), p. 80.
8. W. D. Carey, *Science* 215, 139 (1982).
9. Arms Export Control Act, 22 U.S. Code, sect. 2778 (1976).
10. International Traffic in Arms Regulations, *Title 22, Code Fed. Reg.*, parts 121-128 (February 1976).
11. Specifically, the regulations state that an "export" occurs "whenever technical data is *inter alia* disclosed to foreign nationals in the United States (including plant visits and participation in briefing and symposia) (10), sect. 125.03).
12. Export Administration Act of 1979, 50 U.S. Code Appendix, sect. 2401-20 (1979).
13. *Title 15, Code Fed. Reg.*, part 379 (1982).
14. The Supreme Court has not yet decided whether the First Amendment protects the speech of American citizens in foreign countries (*Haig v. Agee*, 453 U.S. 280, 306-310 (1982)).
15. H. Wechsler, *Principles, Politics and Fundamental Law* (Harvard Univ. Press, Cambridge, Mass., 1961), pp. 3-27.
16. A. M. Buckel, *The Supreme Court and the Idea of Progress* (Yale Univ. Press, New Haven, Conn., 1978), pp. 95-96.
17. T. Emerson, *A System of Freedom of Expression* (Random House, New York, 1970), pp. 6-7.
18. *Virginia Pharmacy Board v. Virginia Consumer Council*, 425 U.S. 748 (1976).
19. J. R. Ferguson, *Harv. Civ. Liberties Law Rev.* 16, 519 (1981).
20. ———, *Cornell Law Rev.* 64, 639 (1979).
21. *Ohralik v. Ohio State Bar Assn.*, 436 U.S. 447, 456 (1978).
22. L. Tribe, *American Constitutional Law* (Foundation Press, Mineola, N.Y., 1978).
23. Office of the Secretary of Defense, *Fed. Reg.* 45, 65 014 (1 October 1980).
24. *Snepp v. United States*, 444 U.S. 507 (1980). See also *Haig v. Agee*, 453 U.S. 280 (1981).
25. *Snepp v. United States* (24). One caveat should be noted here. The Court will apply a more rigorous standard of review to governmental restraints imposed on a publisher who has received confidential information from a government employee (30).
26. Given the government's current emphasis on curbing the transfer of technology, it seems likely that the Department of Defense will be placing an increasing number of contractual restrictions on research that it supports (3).
27. *First National Bank of Boston v. Bellotti*, 435 U.S. 765 (1978).
28. *Schenck v. United States*, 249 U.S. 47 (1919).
29. *New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam). In the *Pentagon Papers* case, the Court found that the government's claims of grave harm to the national security were insufficient to justify a prior restraint on the publication of a classified history of U.S. activities in Vietnam.
30. *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).
31. *Nebraska Press Association v. Stuart*, 427 U.S. 539, 562 (1976).
32. *Abrams v. United States*, 250 U.S. 616, 630 (1919) (Justice Holmes dissenting).
33. H. Jonas, *Philosophical Essays* (Univ. of Chicago Press, Chicago, 1974).
34. *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 995 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979).
35. The injunction issued in the *Progressive* case was later vacated when a Wisconsin newspaper published the relevant information. As a consequence, the decision was never reviewed by a higher court and its precedential value is uncertain. For a useful discussion of the case and its significance, see M. Cheh, *George Wash. Law Rev.* 48, 163 (1980).
36. G. Kolata, *Science* 217, 1233 (1982).
37. T. Gustafson, *Technol. Rev.* 85 (No. 2), 34 (1982).
38. Export Administration, U.S. Department of Commerce, *116th Report on U.S. Export Controls* (April-September, 1977) Appendix D, p. 128.
39. Department of Energy, *Fed. Reg.* 45, 65152 (1 October 1980).
40. E. Mansfield, A. Romeo, M. Schwartz, D. Teece, S. Wagner, P. Brach, *Technology Transfer, Productivity and Economic Policy* (Norton, New York, 1982).
41. This point was demonstrated during World War II when Allied scientists worked to develop the atomic bomb before the Nazis. See C. P. Snow, *The Physicists* (Little, Brown, Boston, 1981), pp. 104-105.
42. *In re Primus*, 436 U.S. 412 (1978).
43. *Central Hudson Gas & Electric Co. v. Public Service Commission*, 447 U.S. 557 (1980).
44. House of Representatives bill H.R. 109 (1981).

**Harvard Civil Rights
Civil Liberties Law Review**



Vol. 16, No. 2
Fall, 1981

SCIENTIFIC AND TECHNOLOGICAL EXPRESSION: A PROBLEM IN FIRST AMENDMENT THEORY†

*James R. Ferguson**

Introduction

“What is involved here is information dealing with the most destructive weapon in the history of mankind, information of sufficient destructive potential to nullify the right to free speech, and to endanger the right to life itself.”¹ With these words the district court in *United States v. The Progressive, Inc.*² explained its decision to enjoin the publication of a magazine article on the design of the hydrogen bomb. The order, the first prior restraint issued by a court in the name of national security, was later mooted when another newspaper published the relevant information.³ But despite its uncertain precedential value, the case has broad significance, for it raised for the first

†Research for this paper was supported by the University of Chicago Law School. The author would like to thank Robert W. Bennett, James A. McKenna, and Victor G. Rosenblum for reading an earlier draft of this Article.

*Member, Illinois Bar.

¹ *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 995 (W.D. Wis.), appeal dismissed, 610 F.2d 819 (7th Cir. 1979).

² *Id.* For useful discussions of the *Progressive* case, see Cheh, *The Progressive Case and the Atomic Energy Act: Waking to the Dangers of Government Information Controls*, 48 GEO. WASH. L. REV. 163 (1980); Tribe & Remes, *Some Reflections on the Progressive Case: Publish and Perish?* BULL. ATOMIC SCIENTISTS, March 1980, at 20; Note, *United States v. Progressive, Inc.: The Faustian Bargain and the First Amendment*, 75 NW. U. L. REV. 538 (1980).

³ The district court issued the preliminary injunction on March 9, 1979, and it remained in effect for six months. N.Y. Times, Sept. 18, 1979, at 1, col. 6. Six days after the Seventh Circuit heard oral argument in the case on September 10, 1979, the *Madison Press Connection* published an article containing the same basic information. *Id.* Immediately thereafter, the government moved to dismiss the appeal and to lift the injunction against THE PROGRESSIVE. *Id.*

time⁴ a number of constitutional issues that soon will demand an authoritative resolution.

To begin with, the *Progressive* litigation clearly illustrated the government's broad statutory authority to regulate scientific and technological expression.⁵ More importantly, however, the case also

⁴ There is, however, an earlier case that is worthy of note. In *United States v. Edler Industries, Inc.*, 579 F. 2d 516 (9th Cir. 1978), the defendants challenged on constitutional grounds their conviction for exporting without a license technical data dealing with rocket and missile components. The Ninth Circuit found that the first amendment claim was "colorable" because the licensing requirement interfered only with the "conduct of assisting foreign enterprises to obtain military equipment and related technical expertise." *Id.* at 520-21.

⁵ As the district court noted, the Atomic Energy Act, 42 U.S.C. §§ 2014-2296 (1976), if read literally, empowers the government to control the dissemination of virtually all information dealing with either nuclear weapons or nuclear energy, information that is deemed to be "restricted data" even if it is conceived or legally gathered by private citizens. 467 F. Supp. at 994. The Act, which provides criminal penalties, 42 U.S.C. § 2274 (1976), states:

The term "Restricted Data" means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 2162 of this title.

Id. § 2014(y). See also Cheh, *supra* note 2, at 176-93.

In a similar vein, other statutes confer on the government a regulatory authority over certain forms of intellectual property. For example, the Invention Secrecy Act, 35 U.S.C. §§ 181-88 (1976 & Supp. III 1979), authorizes the heads of federal agencies to impose a "secrecy order" on patent applications if the agency determines that disclosure "would be detrimental to the national security." *Id.* § 181.

In addition, the State and Commerce Departments are statutorily empowered to control the export of certain technological information. Under the Arms Export Control Act, 22 U.S.C. § 2778 (1976), the State Department's Office of Munitions Control regulates the export of technical data that "can be used, or be adapted for use" in the production of restricted arms, or "establishes a new art in an area of significant military applicability. . . ." 22 C.F.R. § 125.01 (1980) (footnotes omitted).

Under the 1979 amendments to the Export Administration Act, 50 U.S.C. App. §§ 2401-20 (Supp. III 1979), the Commerce Department issues licenses for the export of technical information that is subject to both military and civilian applications. The Department's regulations define "technical data" to include a "model, prototype, blueprint, or an operating manual. . . ." 15 C.F.R. § 379.1 (1981) (footnotes omitted).

For a critical study of the Atomic Energy Act, the Invention Secrecy Act, and the current efforts of the government to monitor the publication of cryptography research, see COMMITTEE ON GOVERNMENT OPERATIONS, *THE GOVERNMENT'S CLAS-*

revealed the ways in which this kind of information can differ from other varieties of speech, and thus pose novel problems for first amendment analysis.⁶ This point was underscored when the government argued that scientific and technological data often do not warrant the same degree of first amendment protection as other types of expression.⁷ The claim rested in large part on the intuitive notion that a technical weapons blueprint should not stand on an equal constitutional plane with a political tract, a work of literature, or a declaration of personal belief. But the argument also drew a measure of support from recent Supreme Court decisions that adopt a hierarchical view of the first amendment, a view that assigns different levels of constitutional protection to different categories of speech.⁸ For example, the Court has held that commercial information warrants only a "limited measure of protection" because it differs in important ways from other types of expression.⁹

The issues raised in the *Progressive* litigation suggest that the time has come for a comprehensive assessment of the constitutional status of scientific and technological information.¹⁰ The purpose of this Article is to fit the broad category of scientific speech within the current framework of established first amendment law.¹¹ The Article will ini-

SIFICATION OF PRIVATE IDEAS, H.R. REP. NO. 96-1540, 96th Cong., 2d Sess. (1980) [hereinafter cited as HOUSE REPORT].

⁶ 467 F. Supp. at 993-97.

⁷ Tribe & Remes, *supra* note 2, at 23.

⁸ See, e.g., *Friedman v. Rogers*, 440 U.S. 1, 10 (1979); *FCC v. Pacifica Foundation*, 438 U.S. 726, 746-47 (1978); *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 455-59 (1978); *Young v. American Mini Theatres, Inc.*, 427 U.S. 50, 70-71 (1976). See also Farber, *Content Regulation and the First Amendment: A Revisionist View*, 68 GEO. L.J. 727 (1980).

⁹ *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978). See generally Jackson & Jeffries, *Commercial Speech: Economic Due Process and the First Amendment*, 65 VA. L. REV. 1 (1979); Farber, *Commercial Speech and First Amendment Theory*, 74 NW. U. L. REV. 372 (1979).

¹⁰ For a brief earlier treatment of the subject, see Ferguson, *Scientific Inquiry and the First Amendment*, 64 CORNELL L. REV. 639, 644-48 (1979).

¹¹ Unless otherwise indicated, this Article will refer to both scientific and technological information as "scientific speech." This is not to suggest, however, that the historic distinction between science and technology is without foundation. According to that view, science seeks to increase the understanding of natural behavior, while technology seeks to increase the efficiency of human activity through machines and other artifacts. Thus, "basic research" is differentiated from "applied research" and

tially explore the unique nature of scientific knowledge as a form of human expression that carries far-reaching implications not only for the realm of ideas but also for the material world. The Article will then rely upon the guidelines established by the Supreme Court in the commercial speech cases to determine the constitutional status of scientific expression. After establishing that scientific expression warrants full constitutional protection, the Article will apply standard first amendment doctrine to a number of constitutional problems involving state-imposed restrictions on scientific speech.

I. The Problem Posed

Traditional views of the modern scientific endeavor often describe a logical continuum of knowledge that is bounded on one end by the concepts of basic science and on the other end by the data of technological development.¹² Granting the validity of this conception, the question arises: why should this body of knowledge be viewed any differently from most other forms of human expression? The answer lies in a single attribute of scientific knowledge: its capacity to confer powers that can alter the material conditions of life.¹³ This feature of

"technological development" on the grounds that the investigator's sole aim is to increase scientific knowledge without regard to its social utility.

In the twentieth century, however, science and technology have become increasingly merged in a "science-based technology" that uses "pure and applied science to build artifacts, construct techniques and organize activities." G. KNELLER, *SCIENCE AS A HUMAN ENDEAVOR* 266 (1978). Indeed, one can now identify a logical continuum that links basic scientific research to applied research, and ultimately to technological application. D. GREENBERG, *THE POLITICS OF PURE SCIENCE* 8-9 (1967). This continuum, however, cannot be sharply divided into neat categories, nor is it always possible to classify a given body of information as "scientific" or "technological." Advances in applied research sometimes open up new fields in basic science, while discoveries in basic research sometimes have immediate practical applications. G. KNELLER, *supra*, at 268; Teller, *The Role of Applied Science*, in *BASIC RESEARCH AND NATIONAL GOALS* 257, 258-60 (Nat'l Acad. Sci. ed. 1965).

¹² See note 11 *supra*. See also Grobstein, *The Recombinant-DNA Debate*, 237 *SCIENTIFIC AM.*, July 1977, at 22, 32.

¹³ H. JONAS, *Technology and Responsibility: Reflections on the New Tasks of Ethics*, in *PHILOSOPHICAL ESSAYS* 3-20 (1974); Ferguson, *supra* note 10, at 644-48.

It is, of course, true that advances in economic theory and other disciplines of human learning sometimes have applications that affect the conditions of everyday life. What is particularly distinctive about scientific advances, however, is that they

scientific information carries a far-reaching significance for first amendment analysis, a significance that becomes clear when the major assumptions of prevailing first amendment theory are briefly examined.

According to established views, the right of free speech is worthy of constitutional protection in part because it promotes a number of important values, such as autonomy, rational decisionmaking, and informed self-government.¹⁴ This fact alone, however, does not fully distinguish speech from various other kinds of social, political, and economic activity.¹⁵ What is equally important, therefore, is the distinctive way in which speech normally contributes to such values. Specifically, unlike other forms of human behavior, the act of individual expression generally depends for its effect on the agreement of others.¹⁶ Thus in the paradigmatic case of "pure speech" the speaker communicates a message in order to persuade others to adopt a particular position or point of view. The listeners, however, are free to accept or reject the speaker's ideas after independently assessing their merit. As a consequence, speech is traditionally viewed as a *noncoercive* activity that does not interfere with the rights or physical welfare of the public.¹⁷

often make possible capabilities of such a "qualitatively novel nature" as to broaden significantly the potential range of human action. H. JONAS, *supra*, at 2.

¹⁴ T. EMERSON, *THE SYSTEM OF FREEDOM OF EXPRESSION* 6, 7 (1970).

¹⁵ See Blasi, *The Checking Value in First Amendment Theory*, 1977 AM. BAR FOUNDATION RESEARCH J. 521, 545; Bork, *Neutral Principles and Some First Amendment Problems*, 47 INDIANA L.J. 1, 20-35 (1971). See also notes 50, 70, & 82 *infra*.

¹⁶ Baker, *Scope of the First Amendment Freedom of Speech*, 25 U.C.L.A. L. REV. 964, 997-1000 (1978).

There are also a number of factors that are frequently considered in determining whether a particular act of expression is constitutionally protected. These factors include the veracity of the message, see *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n*, 447 U.S. 557, 563-64 (1980), and its context. Indeed, John Hart Ely has argued that "context—the threat the particular expressive event poses" will sometimes be dispositive of the constitutional inquiry. J. ELY, *DEMOCRACY AND DISTRUST* 110 (1980). See also L. TRIBE, *AMERICAN CONSTITUTIONAL LAW* § 12-2 (1978); Ely, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 HARV. L. REV. 1482-1508 (1975).

¹⁷ Baker, *supra* note 16, at 999. As a general matter, "speech harms occur only to the extent people 'mentally' adopt perceptions or attitudes." *Id.* at 998. There are, however, certain forms of pure speech that directly produce a tangible harm to oth-

Lying at the heart of this theory is a sharp distinction between the realm of ideas and the material world of action, a distinction based on the intuitive perception that ideas are not harmful in any physical sense.¹⁸ This is a key distinction in first amendment analysis, for it effectively divides the entire range of human behavior into two broad categories, protected "expression" and unprotected "conduct."¹⁹ Under this view, the first amendment generally prohibits official restraints on the communication of ideas, but does not in any way prevent the state from restricting the acts of an individual that may cause physical harm to others.²⁰

ers. Such harms generally result either from the content of the speech or from the manner in which the message is conveyed. See J. ELY, *supra* note 16, at 111-16; L. TRIBE, *supra* note 16, § 12-2. Examples of speech with immediately harmful content include obscenity, fighting words, and libel. Traditionally, the Court has treated such speech as simply outside the scope of first amendment protection. *E.g.*, *Gertz v. Welch*, 418 U.S. 323 (1974) (defamation of private individuals); *Paris Adult Theater I v. Slaton*, 413 U.S. 49 (1973) (obscenity); *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942) (fighting words). *But see* *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964) (defamation of public figures protected unless malicious falsehood). Harms caused by the manner in which a message is conveyed may be prevented by narrowly drawn time, place, and manner regulations. *E.g.*, *Grayned v. City of Rockford*, 408 U.S. 104, 116 (1972); *Cox v. New Hampshire*, 312 U.S. 569 (1941).

¹⁸ Baker, *supra* note 16, at 997-98. Actions, of course, can also express ideas, and therefore can also depend for their effect on the consent of others. *E.g.*, *Spence v. Washington*, 418 U.S. 405 (1974). See Ferguson, *supra* note 10, at 649-50. Moreover, as Professor Tribe has noted, "Expression and conduct, message and medium, are . . . inextricably tied together in all communicative behavior; expressive behavior is 100% action and 100% expression." L. TRIBE, *supra* note 16, § 12-7. See also Ely, *supra* note 16, at 1496 ("Burning a draft card to express one's opposition to the draft is an undifferentiated whole, 100% action and 100% expression. . . ."); Henkin, *The Supreme Court, 1967 Term—Foreword: On Drawing Lines*, 82 HARV. L. REV. 63, 79 (1968) ("A constitutional distinction between speech and nonspeech has no content. . . . Speech is conduct, and actions speak.") (emphasis in the original).

¹⁹ T. EMERSON, *supra* note 14, at 8. See also *Haig v. Agee*, 101 S. Ct. 2766, 2783 (1981); *Zemel v. Rusk*, 381 U.S. 1, 16-17 (1965). *But see* notes 17-18 *supra*. Professor Baker has modified the distinction to accommodate expressive conduct. Noting that the "essential distinction is solely that 'action' involves coercive or physically interfering conduct," he has argued that the category of protected speech should include "noncoercive, nonviolent, and expressive nonverbal conduct." Baker, *supra* note 16, at 1011, 1040.

²⁰ T. EMERSON, *supra* note 14, at 8.

In the case of scientific knowledge, however, the usually sharp distinction between the realm of ideas and the physical world of action does not always hold true. By revealing the explanation for the behavior of natural phenomena, scientific advances often confer the power to alter the conditions of everyday life in new and fundamental ways.²¹ This capacity for technological development is, of course, a source of great benefits to modern society. But it is also a source of potential hazards, for it occasionally introduces new forms of "conduct" that pose dangers to the public.²² Thus, in contrast to most other varieties of speech which affect only the mind of the listener, scientific information can provide nations and individuals with the capability of committing harmful acts that they would not otherwise be able to commit.²³

Yet even this key qualitative difference does not fully explain the difficulties that scientific speech can pose for conventional first amendment analysis. What is equally important is the *magnitude* of the powers that are sometimes conferred by scientific achievements, powers of such a nature and scale as to pose unprecedented dangers.²⁴ This fact was first demonstrated when advances in nuclear physics bestowed on humanity the capacity for global annihilation. So fateful was the acquisition of this capability that it stands even today as the leading symbol of the hazards of twentieth century science. But the same theme is also evident in other areas in which scientists are acquiring the ability to modify the most fundamental physical and biological processes.

To begin with, humanity's intervention in nature has proceeded at such a rate, and to such an extent, that the environment is no longer immune to human activity.²⁵ This development was not fully recog-

²¹ Ferguson, *supra* note 10, at 641-42; Jonas, *Freedom of Scientific Inquiry and the Public Interest*, HASTINGS CENTER REP., Aug. 1976, at 15-16.

²² H. JONAS, *supra* note 13, at 8-19.

²³ Thomas Scanlon has made essentially the same point by emphasizing "the distinction between expression which moves others to act by pointing out what they take to be good reasons for action and expression which gives rise to action by others in other ways, e.g., by providing them with the means to do what they wanted to do anyway." Scanlon, *A Theory of Freedom of Expression*, 1 PHIL. & PUB. AFF. 204, 212 (1972).

²⁴ H. JONAS, *supra* note 13, at 8-19.

²⁵ *Id.* at 9-10.

nized until it began to show itself in the damage that had already been done: the pollution of the air by industrial emissions, the degradation of the land by toxic chemicals, and the destruction of life forms by pesticides and defoliants. These incidents of lasting injury to the biosphere have demonstrated that the permanence of nature can no longer be taken for granted. On the contrary, the environment is so vulnerable to current forms of human intervention that nature has become a human responsibility, a matter committed in trust to the care of the present generation for the benefit of future humanity.²⁶

Nor is the environment the only area of human intervention, for modern science is also acquiring the ability to modify the basic terms of the human condition. Most significant in this regard are two fields of current investigation that promise to provide tools for reshaping both human nature and biological destiny. First, neurobiologists are exploring ways to modify mood, behavior, and personality through the alteration of neurochemical processes and other techniques of neurological intervention.²⁷ Second, molecular biologists are utilizing the recently acquired recombinant DNA technology to develop modes of modifying both the genetic constitution of individuals and the gene pool of the entire species.²⁸

These emerging biological technologies carry a variety of potentially grave implications for the societies that choose them. In the first place, there is no guarantee that such fundamental powers can be managed without committing a grievous biological blunder. It seems doubtful, after all, that a reliable body of knowledge will be available to chart the course of future evolution or guide the modification of human nature.²⁹ In addition, the widespread application of such technologies may lead to unwanted social, political, or economic changes. For example, according to some critics, a major life-extension technol-

²⁶ *Id.*

²⁷ See generally J. DELGADO, *PHYSICAL CONTROL OF THE MIND* (1969).

²⁸ See generally C. GROBSTEIN, *A DOUBLE IMAGE OF THE DOUBLE HELIX* (1979); Grobstein, *supra* note 12.

²⁹ H. JONAS, *supra* note 13, at 17. The ability to manage intelligently the powers conferred by new technologies has been an underlying issue of the recombinant DNA debate. In large measure, the question has arisen because recombinant technology can breach the genetic barrier between species and thus confer novel properties on life forms. See C. GROBSTEIN, *supra* note 28, at 85; Grobstein, *supra* note 12, at 25-29.

ogy could produce a serious social dislocation by aging the general population, and shifting economic and political power to those who are over sixty-five years of age.³⁰

Finally, the acquisition of biological capabilities that promise to alter what were once considered the fixed terms of human nature will undoubtedly raise a variety of ethical problems. One concern, for example, is that the new technologies will displace inherited notions of the "human person as a unique and intrinsically valuable entity, conscious of its own being and responsible for its own choices."³¹ Professor Tribe writes:

[A]s one's most intimate nature as a person—one's genetic basis and neurological identity—becomes increasingly subject to deliberate external manipulation and even prior determination, one's ability to conceive of oneself as a free and rational being entitled to resist various societal claims may gradually weaken and might finally disappear altogether.³²

Thus, Professor Tribe and others suggest that the emerging biological technologies portend the "final transformation of man into an object—a thing to be 'engineered' according to technical specifications along with many other products of human ingenuity."³³

In sum, the twentieth century has witnessed a major change in the nature and magnitude of the powers conferred by scientific knowledge, and so too a major change in the magnitude of the dangers posed by the misuse of that knowledge. Given this reality, it is not surprising that some observers are now calling for restraints on scientific

³⁰ See, e.g., Morison, *Misgivings about Life-Extending Technology*, DAEDALUS, Spring 1978, at 211; Sinsheimer, *Inquiring into Inquiry: Two Opposing Views*, HASTINGS CENTER REP., Aug. 1976, at 18; Sinsheimer, *The Presumptions of Science*, DAEDALUS, Spring 1978, at 23.

³¹ Tribe, *Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality*, 46 S. CAL. L. REV. 617, 648 (1973). For critical studies of the effects of modern technology on the nature of human values, see L. MUMFORD, *THE PENTAGON OF POWER* (1970), and J. ELLUL, *THE TECHNOLOGICAL SOCIETY* (1964).

³² Tribe, *supra* note 31, at 648.

³³ *Id.* at 649.

and technological information as a prudent means of preventing the acquisition of particular capabilities.³⁴ This argument is frequently advanced by the government as part of an effort to curb the proliferation of nuclear arms and other weapons technologies that pose obvious hazards to national security.³⁵ But the same argument is also made in response to emerging biological technologies that may produce distant hazards which are not yet fully recognized.³⁶ In both cases, the essential point is the same: once the relevant knowledge is freely disseminated and developed, the surest safeguard against the dangers resulting from its misapplication is lost forever.

If such arguments are translated into constitutional terms, they effectively frame an important first amendment issue that has not yet been fully addressed. Does scientific information stand on an equal footing with more traditional varieties of pure speech, or does it occasionally warrant a different constitutional approach? The question is especially important in view of the Supreme Court's recent treatment of another class of expression that can cause harms in the physical world, commercial advertising.

In *Virginia Pharmacy Board v. Virginia Consumer Council*,³⁷ the Court broke with precedent³⁸ and held that commercial information falls within the scope of the first amendment's protections.³⁹ At the same time, however, the Court recognized that commercial advertising differs from other types of expression in several important ways, not the least of which is its susceptibility to fraudulent, deceptive, or misleading uses.⁴⁰ For this reason, the Court has held, in cases following

³⁴ See notes 35-36 *infra*.

³⁵ *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 995 (W.D. Wis.), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979). See also note 5 *supra* and statutes cited therein (statutes designed to restrain publication of technical data having military applications).

³⁶ See generally H. JONAS, *supra* note 13; Jonas, *supra* note 21; Sinsheimer, *Inquiring into Inquiry*, *supra* note 30; Sinsheimer, *The Presumptions of Science*, *supra* note 30.

³⁷ 425 U.S. 748 (1976).

³⁸ See note 43 *infra*.

³⁹ 425 U.S. at 770.

⁴⁰ *Id.* at 771 n. 24. See also *Friedman v. Rogers*, 440 U.S. 1, 12-13 (1979) (trade names may be deceptive); *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978) (citing examples of how commercial speech can be harmful).

Virginia Pharmacy,⁴¹ that accurate commercial information warrants only a "limited measure" of constitutional protection against governmental efforts to regulate its use.⁴²

By illustrating the Court's approach to a well-defined category of expression, the commercial speech cases offer a useful frame of reference in determining the constitutional status of scientific expression. The cases are especially relevant since business advertising and scientific information are both occasionally subject to uses that can cause a material harm to others. Accordingly, it is useful to begin the inquiry by examining more closely the analytical guidelines established by the Court in determining the constitutional status of commercial speech.

II. The Commercial Speech Cases

At one time, the Supreme Court viewed commercial advertising as simply another form of economic activity that was properly subject to regulation by majoritarian legislatures.⁴³ However, in the *Virginia Pharmacy* opinion, the Court departed from its earlier decisions, and held that commercial information is sufficiently akin to other varieties of expression to warrant some degree of constitutional protection.⁴⁴ In reaching this conclusion, the Court stressed that commercial speech promotes the three major interests that lie at the core of the first amendment: an individual interest in self-expression; a social interest in the free flow of information and ideas; and a political interest in enlightened public decisionmaking.⁴⁵

The Court began its inquiry with the recognition that both the advertiser and the consumer have a substantial individual interest in

⁴¹ *E.g.*, *Metromedia, Inc. v. City of San Diego*, 101 S.Ct. 2882 (1981); *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n*, 447 U.S. 557 (1980); *Friedman v. Rogers*, 440 U.S. 1 (1979); *Ohralik v. Ohio State Bar Ass'n.*, 436 U.S. 447 (1978).

⁴² *Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n*, 447 U.S. 557 (1980). The Court has formulated a four-part test for determining whether or not commercial speech is protected by the first amendment. See text accompanying note 67 *infra*.

⁴³ See, *e.g.*, *Beard v. City of Alexandria*, 341 U.S. 622 (1951); *Valentine v. Chrestensen*, 316 U.S. 52 (1942).

⁴⁴ 425 U.S. at 771 n.24.

Id. at 761-65.

the communication of commercial data. The advertiser seeks to convey price and product information to the widest possible range of potential customers, and the consumer seeks to learn of the availability of goods at reasonable prices.⁴⁶ The Court then noted that commercial speech also has an important social value because the efficient allocation of resources depends on "intelligent and well informed" private economic decisions.⁴⁷ Finally, in response to Alexander Meiklejohn's theory,⁴⁸ the Court carried its analysis a step further, declaring that if commercial information

is indispensable to the proper allocation of resources in a free enterprise system, it is also indispensable to the formation of intelligent opinions as to how that system ought to be regulated or altered. Therefore, even if the First Amendment were thought to be primarily an instrument to enlighten public decision-making in a democracy, we could not say that the free flow of information does not serve that goal.⁴⁹

Based on this line of analysis, the Court found that commercial speech has an important first amendment value and is thus entitled to some constitutional protection.⁵⁰

Since the *Virginia Pharmacy* decision, however, the Court has consistently held that commercial information warrants only a "limited measure of protection."⁵¹ This standard is based in part on the "subordinate position" that commercial speech holds in the "scale of First Amendment values,"⁵² and in part on certain "commonsense differences" between commercial information and other forms of expression.⁵³ In particular, the Court has found that all forms of commercial

⁴⁶ *Id.* at 762-64.

⁴⁷ *Id.* at 765.

⁴⁸ *Id.* at 765 n.19. See generally A. MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948).

⁴⁹ 425 U.S. at 765 (footnotes omitted).

⁵⁰ *Id.* at 770.

⁵¹ *Ohrlik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978).

⁵² *Id.*

⁵³ *Id.* at 455-56; *Virginia Pharmacy Bd. v. Virginia Consumer Council*, 425 U.S. 748, 771 n.24 (1976). It is not clear from the Court's opinions if these two factors are

speech are "more objective, hence more verifiable than other varieties of speech;"⁵⁴ that they are "less likely than other forms of expression to be inhibited by proper regulation;"⁵⁵ and that they occur "in an area traditionally subject to government regulation."⁵⁶

What underlies the last point is the Court's recognition that commercial information is "linked inextricably to commercial activity" and is therefore more susceptible than most other types of expression to uses that can cause an economic harm to the public.⁵⁷ Accordingly, the Court has upheld a number of state restrictions on forms of commercial speech that are not inherently misleading, but nevertheless give rise to risks of fraud or deception. For example, in *Ohralik v. Ohio State Bar*⁵⁸ the Court rejected the first amendment challenge of an attorney who had been disciplined by the state bar association for personally soliciting potential tort plaintiffs. In so doing, the Court emphasized the considerable risks of harm that are posed by such forms of client solicitation:

The detrimental aspects of face-to-face selling even of ordinary consumer products have been recognized and addressed by the Federal Trade Commission, and it hardly need be said that the potential for overreaching is significantly greater when a lawyer, a professional trained in the art of persuasion, personally solicits an unsophisticated, injured, or distressed lay person. Such an individual may place his or her trust in a lawyer, regardless of the latter's qualifications or the individual's actual need for legal representation, simply in response to persuasion under circumstances conducive to uninformed acquiescence.⁵⁹

distinct, and if so, whether they are of equal significance in the determination of the proper standard of review.

⁵⁴ *Friedman v. Rogers*, 440 U.S. 1, 10 (1979).

⁵⁵ *Id.*

⁵⁶ *Ohralik v. Ohio State Bar Ass'n*, 436 U.S. 447, 456 (1978). See also *Jackson & Jeffries*, *supra* note 9, at 38-39.

⁵⁷ *Friedman v. Rogers*, 440 U.S. 1, 10 n.9 (1979).

⁵⁸ 436 U.S. 447 (1978).

⁵⁹ *Id.* at 464-65 (citations omitted).

The Court thus found an adequate justification for the disciplinary action in the state's reasonable belief that "in-person solicitation by lawyers more often than not will be injurious to the person solicited."⁶⁰

Similarly, in *Friedman v. Rogers*⁶¹ the Court cited the risk of material harm in rejecting a first amendment challenge to a Texas statute that prohibited the practice of optometry under a trade name. The Court noted that, unlike other types of commercial speech, a trade name does not have an intrinsic meaning; rather, "it acquires meaning over a period of time by associations formed in the minds of the public between the name and some standard of price or quality."⁶² Such "ill-defined associations," the Court continued, give rise to a "significant possibility that trade names will be used to mislead the public."⁶³ For example, an unscrupulous practitioner could "assume a new trade name if negligence or misconduct casts a shadow over the old one."⁶⁴ Accordingly, the Court found a "substantial and well-demonstrated" state interest in protecting the public from the deceptive use of trade names, and upheld the statute as a permissible regulation in furtherance of that interest.⁶⁵

Thus, while the Court has been willing to extend a measure of constitutional protection to business advertising, it has not ignored the important differences that separate commercial speech from other types of expression. On the contrary, the Court has recognized that all forms of commercial information share certain characteristics such as objectivity, hardiness, and the potential for deceptive use.⁶⁶ In the light of these differences, the Court has applied to restrictions on business advertising an intermediate standard of review that extends only a "limited measure of protection" to commercial speech.⁶⁷ Under that standard a specific body of commercial data is deemed to be constitutionally protected only if it "concerns lawful activity" and "is not mis-

⁶⁰ *Id.* at 466.

⁶¹ 440 U.S. 1 (1979).

⁶² *Id.* at 12.

⁶³ *Id.* at 12-13.

⁶⁴ *Id.* at 13.

⁶⁵ *Id.* at 15.

⁶⁶ *See id.* at 10.

⁶⁷ *Central Hudson Gas v. Public Serv. Comm'n*, 447 U.S. 557, 566 (1980). *See Metromedia, Inc. v. City of San Diego*, 101 S. Ct. 2882, 2892-95 (1981) (plurality opinion).

leading."⁶⁸ Furthermore, even if these requirements are met, the government can still regulate the information if the asserted state interest is "substantial" and if the regulatory means are "not more extensive than is necessary to serve that interest."⁶⁹

III. The First Amendment Value of Scientific and Technological Speech

If the guidelines established by the Court in the commercial speech cases are followed, an inquiry into the constitutional status of scientific and technological information must begin by determining the first amendment value of scientific speech. In particular, the inquiry must address the ways in which scientific expression promotes three core values of the first amendment: the individual interest in self-expression, the social interest in the free flow of information and ideas, and the political interest in informed self-government.

A. *The Individual Interest in Free Scientific Expression*

A familiar justification for the free speech guarantee is that "some speech activities should be immune from government regulation as a matter of individual right rather than social policy. . . ."⁷⁰ According to this theory, the right of free speech is a basic attribute of liberty because individual expression often serves as a mode of personal fulfillment.⁷¹ The theory thus rests on the widely accepted notion that the individual can best realize his or her character and potential through the uniquely human ability to communicate opinions, beliefs, and ideas.⁷²

Such a conception of the value of free expression clearly applies to scientific communications because they represent the final product in a creative intellectual process. The scientist-in-training must undergo

⁶⁸ 447 U.S. at 566.

⁶⁹ *Id.*

⁷⁰ See Blasi, *supra* note 15, at 544 (footnote omitted). See also R. DWORKIN, *TAKING RIGHTS SERIOUSLY* 190-91 (1978); T. EMERSON, *supra* note 14, at 6; Emerson, *Toward a General Theory of the First Amendment*, 72 *YALE L.J.* 877, 879 (1963).

⁷¹ T. EMERSON, *supra* note 14, at 6; Emerson, *supra* note 70, at 879.

⁷² T. EMERSON, *supra* note 14, at 6.

years of intensive study to master the body of acquired knowledge in his or her chosen field of specialization. When this groundwork is laid the scientist is in a position to identify a problem that warrants investigation, for example, a natural occurrence or phenomenon that is not adequately explained by current theory.⁷³ Once a problem is defined, the scientific endeavor proceeds in two episodes of thought: the imaginative and the critical.⁷⁴ In the imaginative phase, the scientist forms a hypothesis to explain the phenomenon under investigation. The hypothesis is often conceived in a "private moment of illumination,"⁷⁵ a flash of intuition that calls into play the creative qualities of the mind.⁷⁶ In the critical phase, the scientist also engages in creative activity by designing an experimental procedure to test the validity of the hypothesis.⁷⁷ Additionally, to ensure the integrity of the experimental results, the scientist makes use of specific craft skills, such as the proper use of laboratory equipment, the correct reading of instruments, and the accurate appraisal of data.⁷⁸

⁷³ Alternatively, the researcher might simply gather facts or engage in other activities that do not entail the formation of hypotheses. G. KNELLER, *supra* note 11, at 99.

⁷⁴ P. MEDAWAR, *INDUCTION AND INTUITION IN SCIENTIFIC THOUGHT* 46 (1969).

⁷⁵ J. ZIMAN, *PUBLIC KNOWLEDGE: AN ESSAY CONCERNING THE SOCIAL DIMENSION OF SCIENCE* 35-36 (1968).

⁷⁶ Because intuition plays such an important role in the formation of hypotheses, the process has been described as "non-logical." P. MEDAWAR, *supra* note 74, at 56. Nevertheless, it seems clear that certain rational principles or strategies guide scientists in forming and pursuing hypotheses. The two most common forms of scientific reasoning are retrodution and hypothetico-deduction. In the former, the scientist encounters an anomaly, and then reasons to a general principle or explanation that will account for the anomaly. In the latter, the scientist begins with a hypothesis and then deduces general statements or specific predictions from it. G. KNELLER, *supra* note 11, at 113.

⁷⁷ If hypothesis formation is a nonlogical process, see note 76 *supra*, experimentation "lies within and makes use of logic, for it is an empirical testing of the logical consequences of our beliefs." P. MEDAWAR, *supra* note 74, at 46.

⁷⁸ The "craft" aspects of scientific research are discussed in J. RAVETZ, *SCIENTIFIC KNOWLEDGE AND ITS SOCIAL PROBLEMS* 95-101 (1971). As Ravetz notes,

the work of scientific inquiry requires knowledge which is learned only through precept and experience in a multitude of particular cases, and which therefore is not "scientific" in character. The assessment of data and of information, and the manipulation of tools, are all subject to pitfalls; and it is only the craft knowledge of the investigator which

The personal satisfaction arising from such creative intellectual work accounts for much of the scientist's interest in a system of free scientific expression.⁷⁹ But scientists also have strong professional interests in freely disseminating the results of their scientific work.⁸⁰ As Robert K. Merton has shown, institutional science is built on a "reward mechanism" in which professional advancement accrues to those who make "genuinely original contributions to the common stock of knowledge."⁸¹ As a consequence, the scientist's professional standing is largely dependent on peer recognition of his or her originality in specific research endeavors. It is for this reason that bitter disputes over the "priority of discovery" have arisen so frequently in the history of modern science.⁸² And it is for this reason that scientists are so interested in publishing their work before it is anticipated by others.⁸³

The practitioner of science thus has a number of personal and professional interests in freely communicating scientific information

enables him to avoid some and sense the presence of those which remain.

Id. at 101.

⁷⁹ While the above discussion has dealt largely with basic research, it seems clear that applied research and other forms of technological development are equally creative, and thus also serve as a source of personal satisfaction. Indeed, some observers have held that the technological impulse is "closely akin to that of art." Tribe, *supra* note 31, at 641. See Smith, *Art, Technology and Science*, 11 *TECH. AND CULTURE* 493 (1970).

⁸⁰ The scientist's professional interest in free scientific speech might be viewed as roughly akin to an economic interest. In this regard, the Supreme Court has held that the "economic nature" of the individual's interest in free expression does not preclude first amendment protection. See *Virginia Pharmacy Bd. v. Virginia Consumer Council*, 425 U.S. 748, 761 (1976).

⁸¹ R. MERTON, *THE SOCIOLOGY OF SCIENCE* 293 (1973). Merton explains that this "functional emphasis" on originality results from the normative structure of science "which defines originality as a supreme value and thereby makes recognition of one's originality a major concern." *Id.* at 294.

⁸² Indeed, as Merton notes, "almost all of those firmly placed in the pantheon of science—Newton, Descartes, Leibniz, Pascal or Huygens, Lister, Faraday, Laplace or Davy—were caught up in passionate efforts to achieve priority and to have it publicly registered." *Id.* at 334-35.

⁸³ The competitive aspects of modern science are discussed in W. HAGSTROM, *THE SCIENTIFIC COMMUNITY* 69-100 (1965). See generally J. WATSON, *THE DOUBLE HELIX* (1968).

and ideas. When these interests are recognized, it becomes clear that scientific speech is fully consistent with traditional views of self-expression as a mode of personal fulfillment and an attribute of liberty.

B. The Social Value of Free Scientific Expression

In recent decisions the Supreme Court has increasingly invoked the so-called "consequentialist" theory of the free speech right.⁸⁴ According to this theory, the free flow of information and ideas plays an important role in promoting a wide range of desired social ends. Thus, for example, in *Virginia Pharmacy* the Court stressed that the availability of accurate commercial data is crucial to the efficient allocation of resources in a free market system.⁸⁵

Scientific knowledge clearly has an incalculable social value. After all, scientific advances not only contribute to the collective wisdom of the culture, but also make possible practical applications that improve the quality of modern life. The real question, then, is whether a system of free scientific expression, as opposed to an official policy of *selective* suppression,⁸⁶ promotes the discovery of scientific truth.⁸⁷

⁸⁴ E.g., *Virginia Pharmacy Bd. v. Virginia Consumer Council*, 425 U.S. 748, 765 (1976). One corollary of the "social function" theory of the free speech guarantee is the public's first amendment right to *receive* information and ideas. See, e.g., *Procurier v. Martinez*, 416 U.S. 396, 408-09 (1974); *Kleindienst v. Mandel*, 408 U.S. 753, 762-63 (1972). For a discussion of the relative merits of the "consequentialist" and "libertarian" interpretations of the first amendment, see L. TRIBE, *supra* note 16, § 12-1.

⁸⁵ 425 U.S. 748, 765 (1976).

⁸⁶ One historic example of the selective suppression of scientific information is the so-called "Lysenko affair" in which the Soviet Union attempted to accelerate its agricultural program by adopting Lysenko's genetic theories to the exclusion of competing alternatives. See generally Z. MEDVEDEV, *THE RISE AND FALL OF T. D. LYSENKO* (1969).

⁸⁷ As a general matter, the following discussion applies to information and ideas that are the immediate products of basic scientific research. In the case of technological data, the obvious social value of the information arises from the useful capabilities it confers. See text accompanying notes 125-34 *infra*. Additionally, technological advances often facilitate the acquisition of basic scientific knowledge, as is clearly illustrated by the recently-acquired recombinant DNA technology. See note 130 *infra*.

In other words, does the well-known "free market of ideas" theory have any validity in the domain of science?⁸⁸

To answer this question, it is necessary to examine briefly the method of scientific inquiry.⁸⁹ As noted earlier, the work of science begins with the formulation of a hypothesis to explain some imperfectly understood natural phenomenon. The scientist next reasons deductively to determine what consequences would follow logically if the hypothesis were true, and then tests these "predictions" against experimental observation of the actual events in nature. If the predictions are accurate, the hypothesis is confirmed and the scientist publishes the research for critical evaluation by scientific peers. If the predictions are inaccurate, the scientist either revises the hypothesis until accurate predictions result or discards the hypothesis altogether.⁹⁰

Normally, a hypothesis fits within a larger conceptual framework that is shared by scientists in the research field, what Thomas S. Kuhn has termed a "paradigm."⁹¹ As a conceptual model of nature, the par-

⁸⁸ The "free market of ideas" theory holds that "the best test of truth is the power of the thought to get itself accepted in the competition of the market." *Abrams v. United States*, 250 U.S. 16, 630 (1919) (Holmes, J., dissenting). In recent years, however, several scholars have questioned the notion that political or philosophical truth will always prevail over falsehood in a free and open encounter. See, e.g., L. TRIBE, *supra* note 16, § 12-1; Blasi, *supra* note 15, at 549-50; DuVal, *Free Communication of Ideas and the Quest for Truth*, 41 GEO. WASH. L. REV. 161, 188-94 (1972).

⁸⁹ For general discussions of the method of scientific inquiry, see G. KNELLER, *supra* note 11, at 105-19; P. MEDAWAR, *supra* note 74, at 35-59; Ziman, *supra* note 75, at 30-62.

⁹⁰ P. B. Medawar thus writes that scientific reasoning "is a constant interplay or interaction between hypotheses and the logical expectations they give rise to: there is a restless to-and-fro motion of thought, the formulation and rectification of hypotheses, until we arrive at a hypothesis which, to the best of our prevailing knowledge, will satisfactorily meet the case." P. MEDAWAR, *supra* note 74, at 48.

⁹¹ T. KUHN, *THE STRUCTURE OF SCIENTIFIC REVOLUTIONS* 10 (1970). As an alternative to Kuhn's "paradigm," Imre Lakatos has described the theoretical assumptions underlying a specific research tradition as a "research program." Lakatos, *Falsification and the Methodology of Scientific Research Programmes*, in *CRITICISM AND THE GROWTH OF KNOWLEDGE* 155, 179 (I. Lakatos & A. Musgrave eds. 1970). Kuhn himself has suggested that the notion of a "disciplinary matrix" might be a more useful concept than "paradigm." T. KUHN, *supra*, at 182.

As a general matter, the scientific theory that underlies a specific "paradigm" or "research program" identifies observed regularities in nature (which are described in "laws" or empirical generalizations), and postulates a mechanism that accounts for

adigm guides the research endeavor by identifying significant problems and promising avenues of inquiry.⁹² Thus, for example, Darwinian theory has governed fields of modern biology, just as relativity theory has governed areas of twentieth century physics. On occasion, however, a line of investigation will yield a significant body of data that cannot be reconciled with the accepted model.⁹³ The appearance of such "anomalies" marks the beginning of a crisis period in which scientists propose alternative paradigms and debate their respective merits.⁹⁴ This period of theoretical uncertainty continues until one conceptual model captures the field by explaining in persuasive ways the facts that undermined the earlier paradigm.⁹⁵

Lying at the heart of the scientific method, then, is a process of rigorous testing⁹⁶ in which statements, ideas, and theories are published for critical evaluation and thereby exposed to the "hazard of refutation."⁹⁷ On one level, a hypothesis is accepted by scientists only if it squares with the results of independent investigation and measurement.⁹⁸ On another level, a theory or paradigm is accepted by scientists only if it explains the behavior of nature in more plausible ways than competing alternatives. Karl Popper writes:

such regularities. For example, Newtonian physics explains the inverse relationship between the volume and pressure of a gas at constant temperature in terms of the kinetic energy of colliding gas molecules. For a useful discussion of scientific theories as models of mechanisms in nature, see R. HARRÉ, *PRINCIPLES OF SCIENTIFIC THINKING* 33-60 (1970).

⁹² T. KUHN, *supra* note 91, at 35-51. As Kuhn explains it, the paradigm operates as a "vehicle for scientific theory," providing a "map whose details are elucidated by mature scientific research." *Id.* at 109. Such a "map" is essential, in Kuhn's view, because "nature is too complex and varied to be explored at random. . . ." *Id.* at 109.

⁹³ T. KUHN, *supra* note 91, at 52-76.

⁹⁴ *Id.*

⁹⁵ *Id.* at 77-91. It should be emphasized that an established theory or paradigm will not be abandoned by a given scientific field until a more inclusive theory becomes available. *Id.* at 77; Lakatos, *supra* note 91, at 146-59.

⁹⁶ John M. Ziman describes a good experiment as a "powerful piece of rhetoric, [for] it has the ability to persuade the most obdurate and skeptical mind to accept a new idea." J. ZIMAN, *supra* note 75, at 36.

⁹⁷ K. POPPER, *THE LOGIC OF SCIENTIFIC DISCOVERY* 280 (1962). It is in this sense that the publication of a scientific paper is a "formal invitation to criticism." H. JUDSON, *THE SEARCH FOR SOLUTIONS* 11 (1980).

⁹⁸ K. POPPER, *supra* note 97, at 108.

We choose the theory which best holds its own in competition with other theories; the one which, by natural selection, proves itself the fittest to survive. This will be the one which not only has hitherto stood up to the severest tests, but the one which is also testable in the most rigorous way.⁹⁹

Clearly, then, a system of free scientific expression is essential to the operation of the scientific method. The process adopts as its central principle the notion that scientific knowledge is determined by a freely accepted consensus of professional opinion.¹⁰⁰ To this extent, therefore, the method assumes the existence of an autonomous scientific community that serves as the sole judge of scientific merit and the

⁹⁹ *Id.* The above discussion represents a broad outline of what might be described as a consensus view of the way in which science progresses. There is, however, a vast literature on the nature of scientific progress, and a number of conflicting schools of thought.

The oldest theory, and the one that is the most consistent with popular conceptions of the scientific endeavor, is "logical empiricism." According to this "positivist" interpretation, scientists formulate theories using inductive logic. Predictions are then deduced from the theory and experimentally tested to confirm or refute the theory. In this manner, according to the positivists, science progresses logically and inexorably closer to the truth. See Wade, *Thomas S. Kuhn: Revolutionary Theorist of Science*, 197 SCIENCE 143 (1977).

Karl Popper provided the first major challenge to logical empiricism. Following Hume's critique of inductive logic, Popper argued that the accumulation of evidence can never conclusively prove a scientific theory, because the theory can still be refuted by the next piece of evidence. Popper also held, however, that a theory can be empirically falsified. He therefore claimed that the chief aim of the scientific endeavor is to formulate theories that are falsifiable and to attempt to refute them through experimental testing. K. POPPER, *supra* note 97, at 40-41, 108, 280.

Thomas S. Kuhn has argued that many important advances are achieved during periods of "normal science" in which scientists, working in a common intellectual tradition, develop the implications of the theoretical paradigm that governs the field. In Kuhn's view, a fundamental change in theory occurs only rarely; and when it does occur, nonrational factors play a key role in the "conversion" of scientists to the new paradigm. Kuhn, *supra* note 91, at 23-42.

For a helpful discussion of Kuhn, Popper, and the positivists, see F. SUPPE, *THE STRUCTURE OF SCIENTIFIC THEORIES* 135-51, 167-70 (1977). For a notable recent effort to strike a middle ground between Popper and Kuhn, see Lakatos, *supra* note 91.

¹⁰⁰ J. ZIMAN, *supra* note 75, at 9; Polanyi, *The Republic of Science*, in *CRITERIA FOR SCIENTIFIC DEVELOPMENT* 1-20 (E. Shils ed. 1968).

final arbiter of scientific disputes.¹⁰¹ Furthermore, because it relies so heavily on critical evaluation as a means of exposing error, the scientific method seeks to test theories and propositions against the widest possible range of independent investigations.¹⁰² Accordingly, the dissenting opinions of critically thinking scientists "are not merely tolerated; they are warmly welcomed and, if successful, richly rewarded."¹⁰³

There is, moreover, another way in which a system of free scientific expression promotes the discovery of scientific truth: it provides an ever increasing fund of "public knowledge" that enables scientists to benefit from the work of colleagues.¹⁰⁴ This is particularly significant in view of the corporate and collective nature of the scientific enterprise.¹⁰⁵ Unlike art and other forms of human creativity, scientific achievements do not exist as separable entities, but are "parts of a single edifice that is collectively assembled by scientists."¹⁰⁶ Accordingly, as John M. Ziman has noted,

[A] scientist does not merely rely upon his apparatus, his eyes and his own logical powers; to an enormous extent he relies upon other people, through their published work, through the results of their experiments, through the techniques that they have initiated and tested, through the theories that they have originated and developed. The 'bibliog-

¹⁰¹ Thomas S. Kuhn writes:

The very existence of science depends upon vesting the power to choose between paradigms in the members of a special kind of community. Just how special that community must be if science is to survive and grow may be indicated by the very tenuousness of humanity's hold on the scientific enterprise. . . . [O]nly the civilizations that descend from Hellenic Greece have possessed more than the most rudimentary science. The bulk of scientific knowledge is a product of Europe in the last four centuries. No other place and time has supported the very special communities from which scientific productivity comes.

T. KUHN, *supra* note 91, at 167-68.

¹⁰² J. ZIMAN, *RELIABLE KNOWLEDGE* 7, 59 (1978).

¹⁰³ *Id.* at 131.

¹⁰⁴ This point is fully developed in J. ZIMAN, *supra* note 75.

¹⁰⁵ Weisskopf, *Art and Science*, 48 AM. SCHOLAR 473, 480 (1979).

¹⁰⁶ *Id.* at 477; J. ZIMAN, *supra* note 75, at 58-59.

raphy' of a scientific paper is a clear and explicit recognition of this dependence.¹⁰⁷

Thus, a widely hailed achievement, or a seemingly insignificant piece of evidence, can inspire others to pursue new lines of investigation yielding yet additional knowledge. In this manner, the publication of scientific papers achieves a "corporate, collective power that is far greater than any one individual can exert."¹⁰⁸

Thus, for all of the reasons cited above, a system of free scientific expression promotes the discovery of scientific truth and consequently serves a vital social interest.

C. *The Political Interest in Free Scientific Expression*

In his classic work, *Free Speech and Its Relation to Self-Government*,¹⁰⁹ Alexander Meiklejohn set forth a theory of the first amendment that has since become the single most influential interpretation of the free speech guarantee.¹¹⁰ Meiklejohn's theory took as its major premise the claim that the first amendment must be considered as an integral part of the democratic system established by the Constitution.¹¹¹ Once this is granted, he argued, it becomes clear that the "principle of the freedom of speech springs from the necessities of the program of self-government."¹¹² Indeed, Meiklejohn claimed that the sole purpose of the first amendment is to promote enlightened public decisionmaking by insuring that "everything worth saying shall be said."¹¹³

¹⁰⁷ J. ZIMAN, *supra* note 75, at 58-59.

¹⁰⁸ Ziman, *Information, Communication, Knowledge*, 224 NATURE 318-24 (1969).

¹⁰⁹ A. MEIKLEJOHN, *supra* note 48.

¹¹⁰ For examples of Meiklejohn's influence on first amendment scholarship, see Bork, *supra* note 15, at 1; Kalven, *The New York Times Case: A Note on "The Central Meaning of the First Amendment,"* 1964 SUP. CT. REV. 191; Polsby, *Buckley v. Valeo: The Special Nature of Political Speech*, 1976 SUP. CT. REV. 1. For examples of Meiklejohn's influence on the Supreme Court, see *New York Times Co. v. Sullivan*, 376 U.S. 254, 269-70 (1964), and cases cited therein.

¹¹¹ Meiklejohn, *The First Amendment Is an Absolute*, 1961 SUP. CT. REV. 245, 356.

¹¹² A. MEIKLEJOHN, *supra* note 48, at 27.

¹¹³ *Id.* at 26.

He therefore insisted that the free speech guarantee affords an absolute protection not only to "public discussions of public issues," but also to forms of expression that contribute to the electorate's "capacity for sane and objective judgment," for example, literature, philosophy, the arts, and the sciences.¹¹⁴

Meiklejohn's emphasis on the role of the first amendment in promoting intelligent self-government has found its way into the Supreme Court's own interpretation of the free speech guarantee. The Court has agreed that a "major purpose of the First Amendment [is] to protect the free discussion of governmental affairs,"¹¹⁵ and it has endorsed the "principle that debate on public issues should be uninhibited, robust, and wide-open."¹¹⁶ Furthermore, the Court has recognized that public debate must be informed as well as unrestricted.¹¹⁷ Accordingly, the Court has gone beyond Meiklejohn's emphasis on discourse and argumentation to hold that the first amendment also protects the "stock of information from which [citizens] may draw" in forming opinions on matters of public importance.¹¹⁸

The Court's emphasis on the "informational purpose of the First Amendment"¹¹⁹ suggests the ways in which scientific expression fits within a conception of the free speech guarantee as an instrument of enlightened public decisionmaking.¹²⁰ To begin with, as Meiklejohn argued, scientific advances contribute to the nation's capacity for self-government by enhancing the electorate's "knowledge, intelligence [and] sensitivity to human values."¹²¹ More importantly, however, sci-

¹¹⁴ Meiklejohn, *supra* note 111, at 256-57.

¹¹⁵ *Mills v. Alabama*, 384 U.S. 214, 218 (1966). See also *First Nat'l Bank v. Bellotti*, 435 U.S. 765 (1978) (special nature of political speech); *Buckley v. Valeo*, 424 U.S. 1 (1976) (*per curiam*) (same).

¹¹⁶ *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964).

¹¹⁷ See *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 782-83 (1978); *Kleindienst v. Mandel*, 408 U.S. 754, 762 (1972). See also *Saxbe v. Washington Post Co.*, 417 U.S. 843, 862-63 (1974) (Powell, J., dissenting) ("public debate must not only be unfettered; it must also be informed").

¹¹⁸ *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 783 (1978).

¹¹⁹ *Id.* at 782 n.18 (1978).

¹²⁰ It should be noted that one advocate of this interpretation of the free speech guarantee would exclude from the first amendment's protections all forms of expression that are not explicitly political. Bork, *supra* note 15, at 20-35.

¹²¹ Meiklejohn, *supra* note 111, at 256.

entific information has a direct and vital bearing on a wide range of public policy issues. To cite only a few examples, scientific and technological information is essential to the formation of intelligent opinions on the risks and benefits of nuclear power, the merits of a strategic arms limitation agreement; the proposed regulation of recombinant DNA research; the feasibility of a solar energy program; the alleged need for new weapons systems; and the health hazards of herbicides, pesticides, and industrial wastes. Indeed, scientific knowledge is crucial to such an array of specific policy issues that many analysts feel it should play a larger role in the general process of policy formation. For example, with the mounting evidence of biological influences on human social behavior, some observers have called for a biologically informed perspective on public policy, a perspective that draws on biological ideas in much the same way that current perspectives draw on economic theory.¹²² In these ways and many others, then, the free flow of scientific information and ideas is essential to the decisionmaking process in a democratic state.

It is thus clear that a system of free scientific expression promotes each of the three major interests that the Court has identified as first amendment concerns. On this basis, it seems clear that the first amendment value of scientific speech is at least equal to that of any other category of expression. This, however, cannot end the inquiry in determining the constitutional status of scientific speech, for there remains another, and perhaps more difficult question: precisely what significance should be given to the capacity of scientific knowledge to confer powers that are subject to misuse in the physical world?

IV. A Search for an Appropriate Standard

A. Scientific Speech

As noted earlier, in the commercial speech cases the Supreme Court identified a number of "commonsense differences" between commercial speech and other types of information. Specifically, the Court cited the hardiness and objectivity of commercial data, and

¹²² See, e.g., *Tiger, Live People in the Machine Age*, N.Y. Times, May 14, 1978, § E, at 20, col. 1. See also Albin, *Biopolitics: Odd Hybrid or a Synthesis?* N.Y. Times, Aug. 23, 1981, § E, at 7, col. 3.

stressed the risks of harm that are posed by misleading advertising. These differences, together with the diminished first amendment value of commercial information, led the Court to apply an intermediate standard of review to restrictions on business advertising.¹²³

The initial question arising from the Court's approach to commercial speech is whether the broad category of scientific expression can be similarly distinguished from other varieties of speech for purposes of first amendment analysis. The answer is clearly that this category affords no meaningful basis for a different standard of judicial review. It is true that some types of scientific information can be used in ways that pose dangers to the material welfare of others. But this characteristic is not shared by all forms of scientific speech in the same way that commercial data share the characteristics of objectivity, hardness, and the potential for deceptive use. On the contrary, a considerable body of scientific data and ideas contributes to the general understanding of natural phenomena and has no practical significance at all. Accordingly, there is no basis for applying a lower standard of review to the broad category of scientific speech, particularly in view of its substantial first amendment value.

B. Technological Speech

While the broad category of scientific speech does not warrant a lower standard of review, it might be argued that technological forms of scientific information share a distinctive characteristic that justifies a different constitutional treatment. It could thus be said that a limited measure of protection should be given to any body of information having applications that are subject to misuse in the physical world. Such an approach would be appropriate for technological information that is only subject to military applications, for example—technical data on thermonuclear weapons design, such as that involved in the *Progressive* case.¹²⁴ As a general matter, however, technological infor-

¹²³ See text accompanying notes 54–69 *supra*.

¹²⁴ This conclusion is supported by the familiar notion that the "greater power normally includes the lesser." Jackson & Jeffries, *supra* note 9, at 34–35. Specifically, it seems clear that any data that can only be used in a military context has no substantive value apart from its military applications. It seems equally clear that Congress has the authority to outlaw or control the use of specific military technologies by private citizens. Accordingly, if Congress were to exercise this power in a particular

mation can be used in beneficial as well as harmful ways, and this oft-noted fact complicates any effort to justify a lower standard of review.

To take one example, consider the current controversy sparked by recent advances in cryptography research. In the past few years, computer scientists and mathematicians have worked on the development of undecipherable computer communication codes.¹²⁵ This research has attracted the attention of the National Security Agency, apparently because the codes could "greatly inhibit the NSA's intelligence gathering functions" by providing other nations with impenetrable communication systems.¹²⁶ At the same time, however, it is clear that the cryptography advances fulfill an important social need for the secure encryption of computer information. Indeed, with the increasing use of computers as a means of storing sensitive personal, financial, and corporate data, the protection of computer information has become a matter of some urgency.¹²⁷ The unbreakable codes thus promise to have a wide range of uses for banks, corporations, and government agencies.¹²⁸

case, the dissemination of the underlying information could serve no valid purpose, since its only possible use would be prohibited by law.

In some circumstances, it might be argued that the mere publication of the scientific data is itself a political message. For example, Tribe and Remes have suggested that the technical data at issue in the *Progressive* case should be viewed as "political speech" which warrants the highest level of first amendment protection. Tribe & Remes, *supra* note 2, at 22-24. Specifically, they argue that the information acquired by the magazine provided an effective comment on the futility of the government's efforts to maintain the "nuclear secret." *Id.* at 20.

This argument is unpersuasive, however, because the claimed political message arises not from the technical data, but from the fact of its acquisition. Indeed, the same point could have been made with equal force by an affidavit from the Secretary of Energy which confirmed that the information in the magazine's possession was indeed an accurate design of a thermonuclear weapon. It seems clear, therefore, that the data itself had no political significance, and could not be viewed as political speech.

¹²⁵ See generally Kahn, *Cryptology Goes Public*, 58 FOREIGN AFF. 142 (1979). See also HOUSE REPORT, *supra* note 5, at 63-120; Kolata, *New Codes Coming into Use*, 208 SCIENCE 694 (1980); Browne, *Cryptography is Too Good for Anyone's Comfort*, N.Y. Times, June 4, 1978, § E, at 7, col. 3.

¹²⁶ HOUSE REPORT, *supra* note 5, at 62-63. See Kolata, *Prior Restraints on Cryptography Considered*, 208 SCIENCE 1442 (1980); N.Y. Times, Oct. 19, 1977, § A, at 26, col. 1.

¹²⁷ Kolata, *supra* note 125, at 694.

¹²⁸ See *id.*; Browne, *supra* note 125.

The same point is illustrated by the recently acquired recombinant DNA technology. By enabling scientists to piece together genetic material in novel combinations, this technology poses potential hazards of considerable magnitude. For example, some critics have argued that recombinant techniques could provide a terrorist group with the means of cheaply creating an effective weaponry in the form of new epidemic pathogens.¹²⁹ Others have suggested that the recombination of genetic material from different species in self-replicating organisms could lead to a biological crisis by breaching the evolutionary barrier against the interbreeding of species.¹³⁰

At the same time, however, research with recombinant DNA promises to yield an astonishing array of social benefits. It is now clear, for instance, that the new technology will soon be used to produce a wide range of vital substances including "improved vaccines, scarce hormones, specially designed drugs, enzymes and perhaps even food."¹³¹ Indeed, scientists have already achieved some notable triumphs in the use of recombinant techniques to create bacteria that synthesize human hormones such as insulin and somatotropin.¹³² Beyond these immediate benefits, recombinant technology may also herald an era of "true gene therapy," for, according to many scientists, it will eventually enable physicians to correct genetic mutations that are responsible for a broad range of human diseases.¹³³ Finally—and perhaps most importantly—recombinant DNA provides the scientific community with an invaluable research tool that will contribute greatly to a deeper understanding of genetic processes, and thus facilitate yet additional advances in medicine, chemistry, and agriculture.¹³⁴

It seems clear, then, that the social value of technological expression is so substantial that this category of speech cannot be viewed as

¹²⁹ See Grobstein, *supra* note 12, at 31.

¹³⁰ See, e.g., Sinsheimer, *Recombinant DNA—On Our Own*, BIOSIENCE, Oct. 26, 1976, at 599; Sinsheimer, *Troubled Dawn for Genetic Engineering*, NEW SCIENTIST, Oct. 16, 1975, at 148 *passim*. See generally C. GROBSTEIN, *supra* note 28, at 48-50.

¹³¹ N.Y. Times, May 22, 1979, § C, at 2, col. 4. See C. GROBSTEIN, *supra* note 28, at 54-58.

¹³² See N.Y. Times, May 22, 1979, § C, at 2, col. 4; *id.*, Sept. 11, 1979, § C, at 1, col. 4.

¹³³ See *id.*, May 22, 1979, § C, at 2, col. 4; C. GROBSTEIN, *supra* note 28, at 61-62.

¹³⁴ C. GROBSTEIN, *supra* note 28, at 33-65.

warranting less protection than other forms of expression.¹³⁵ If this is granted, it follows that restraints on scientific and technological expression should generally be viewed from a standard first amendment perspective.¹³⁶ In particular, the constitutional inquiry should rely on settled principles of first amendment law to determine if the state's interest in regulating the information at issue is sufficient to justify a restraint on fully protected speech.¹³⁷ Such an approach would not ignore the unique dangers occasionally posed by scientific and technological information; rather, it would address them on a case-by-case basis in weighing the particular state interest in regulation.

V. Restrictions on Scientific Speech: A Constitutional Analysis

A. General Principles

The Supreme Court has consistently held that a statute imposing criminal sanctions or other restrictions on the fully protected "speech of a private person" will be upheld only if the government can show a "compelling" rather than "substantial" interest in regulation.¹³⁸ According to the Court, the strength of the regulatory interest will hinge in large measure on two factors, the gravity of the substantive "evil" that the state is seeking to avert, and the likelihood of its occur-

¹³⁵ Stated differently, given the incalculable social and political value of applied scientific knowledge, it cannot be said that technological expression has the same diminished first amendment value as commercial speech. As noted earlier, the Supreme Court has based its treatment of commercial speech in part on the "subordinate position" that business advertising occupies in the "scale of First Amendment values." See notes 53-55 *supra*, and cases cited therein.

¹³⁶ The one major exception to this general principle is technological data that is subject only to military applications. See text accompanying notes 124-132 *supra*.

¹³⁷ The following discussion does not deal with the transmission of scientific or technological data to a foreign nation as part of an espionage plot, an activity that is plainly not protected by the first amendment. See, e.g., *United States v. Rosenberg*, 195 F.2d 583, 591 (2d Cir. 1952). For a general discussion of the espionage statutes, 18 U.S.C. §§ 792-99 (1976), see Edgar & Schmidt, *The Espionage Statutes and the Publication of Defense Information*, 73 COLUM. L. REV. 929 (1973).

¹³⁸ See, e.g., *Consolidated Edison Co. v. Public Serv. Comm'n*, 447 U.S. 530, 534 (1980); *First Nat'l Bank v. Bellotti*, 435 U.S. 765, 786 (1978); *Buckley v. Valeo*, 424 U.S. 1, 25 (1976) (*per curiam*).

rence.¹³⁹ Under this formulation, the government's burden in showing the "likelihood of occurrence" will decrease as the gravity of the potential danger increases. If this combination of factors provides a "compelling" interest in regulation, the state must then show that it does not have a "less restrictive alternative" to the restraints on speech imposed by the regulatory scheme at issue.¹⁴⁰ Additionally, the state may be required to show that its regulation, particularly if it imposes criminal penalties, is neither impermissibly vague¹⁴¹ nor overly broad.¹⁴²

The state would carry an even heavier burden if it sought a prior restraint on publication. The Court has held that the "presumption against prior restraints is heavier—and the degree of protection is broader—than that against limits on expression imposed by criminal penalties."¹⁴³ Thus, in *New York Times Co. v. United States*,¹⁴⁴ the Court found that the government's interest in preventing the publication of the Pentagon Papers, a classified history of the Vietnam War, was inadequate to justify a prior restraint. The Court's three-paragraph per curiam opinion offered no guidance as to what showing the state must make in order to overcome the heavy presumption against

¹³⁹ Thus, in *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829, 843 (1978), the Court declared that it will "make its own inquiry into the imminence and magnitude of the danger said to flow from the particular utterance and then . . . balance the character of the evil, as well as its likelihood, against the need for free and unfettered expression." *Id.* See *Bridges v. California*, 314 U.S. 252, 271 (1941).

¹⁴⁰ A useful discussion of the "less restrictive alternative" doctrine is furnished by Ely, *supra* note 16. See also Note, *Less Drastic Means and the First Amendment*, 78 YALE L.J. 464 (1969).

¹⁴¹ The Court has required that legislation imposing criminal penalties in the first amendment area display "[p]recision of regulation [that] must be the touchstone in an area so closely touching on our most precious freedoms." *Buckley v. Valeo*, 424 U.S. 1, 41 (1976) (per curiam), quoting *NAACP v. Button*, 371 U.S. 415, 438 (1963).

¹⁴² See *Dombrowski v. Pfister*, 380 U.S. 479, 490-92. See generally Note, *The First Amendment Overbreadth Doctrine*, 83 HARV. L. REV. 844 (1970). The overbreadth doctrine is not applicable to commercial speech cases. See *Bates v. State Bar Ass'n*, 433 U.S. 350, 379-81 (1977).

¹⁴³ *Southeastern Promotions Ltd. v. Conrad*, 420 U.S. 546, 558-59 (1974). Elsewhere, the Court has declared that a prior restraint bears a "heavy presumption" against its constitutional validity. *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971). Accord, *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam).

¹⁴⁴ 403 U.S. 713 (1971) (per curiam).

prior restraints.¹⁴⁵ However, in oft-cited passages from two concurring opinions, Justices Brennan, Stewart, and White stated that they would uphold a prior restraint only if the government could show that a grave and irreparable harm would "surely" or "inevitably" result from publication.¹⁴⁶

Recently, however, a majority of the Court altered this formulation in a subtle but significant way. In *Nebraska Press Association v. Stuart*,¹⁴⁷ the Court considered a constitutional challenge to a judicial order that prohibited the pre-trial publication of information implicating an accused murderer. Writing for the Court, Chief Justice Burger found that the threatened harm to the accused's right to a fair trial was too "speculative" to justify a prior restraint.¹⁴⁸ In defining the appropriate inquiry, however, the Court quoted with approval Judge Learned Hand's test: whether the "gravity of the 'evil,' discounted by its improbability, justified such invasion of free speech as is necessary to avoid the danger."¹⁴⁹ It would thus seem that even in justifying a prior restraint, the government's burden in showing the "likelihood of occurrence" will be lessened if the threatened harm is sufficiently grave.¹⁵⁰

¹⁴⁵ *Id.*

¹⁴⁶ To be more specific, Justice Stewart, joined by Justice White, required a showing that "disclosure . . . will surely result in direct, immediate and irreparable damage to our Nation or its people." *Id.* at 730 (Stewart, J., concurring). Justice Brennan required a showing that "publication [will] inevitably, directly and immediately cause the occurrence of an event kindred to imperiling the safety of a transport already at sea." *Id.* at 726-27 (Brennan, J., concurring). See Cox, *The Supreme Court, 1979 Term—Foreword: Freedom of Expression in the Burger Court*, 94 HARV. L. REV. 1, 6-7 (1980).

¹⁴⁷ 427 U.S. 539 (1976). For a critical discussion, see Schmidt, *Nebraska Press Association: An Expansion of Freedom and Contraction of Theory*, 29 STAN. L. REV. 431 (1977).

¹⁴⁸ 427 U.S. at 563-69.

¹⁴⁹ *Id.* at 562, quoting *United States v. Dennis*, 183 F.2d 201, 212 (2d Cir. 1950).

¹⁵⁰ Such an approach has a considerable appeal to common sense, as Tribe and Remes have noted in their discussion of the *Progressive* case:

Ordinarily, the government may justify a prior restraint only by showing that grave and irreparable harm will *surely* follow publication. Only on this kind of showing may a court enjoin publication on pain of contempt, a far more total restraint on liberty than the mere threat of punishment *after* the fact. No such degree of certainty can defensibly be required, however, when the threatened harm is not some nebulous and intangible injury to the

The above principles would guide the Court in assessing the constitutionality of governmental restraints on the speech of private citizens. A very different problem would arise, however, if the state imposed restrictions on the dissemination of its own information by its own employees.¹⁵¹ In *Snepp v. United States*,¹⁵² for example, a former agent of the Central Intelligence Agency challenged an employment contract in which he had agreed to refrain from publishing any "material relating to the Agency . . . without specific prior approval by the Agency."¹⁵³ In a brief per curiam opinion, the Court rejected the claim, and broadly affirmed the state's power to "protect substantial government interests by imposing reasonable restrictions on employee activities that in other contexts might be protected by the First Amendment."¹⁵⁴ The opinion further declared that this principle would apply "even in the absence of an express agreement" between the government and the employee.¹⁵⁵ Accordingly, in the light of this holding, the government's power to protect the secrecy of information through restraints on employee communications is bounded only by considerations of "reasonableness."

By the same token, the state would be accorded considerable latitude in imposing restraints on private parties as a condition on the receipt of public funds for the conduct of research. Indeed, in such a case, the government's restrictions on speech could usually be upheld on either of two grounds: the government, by financing the underlying research, acquires a property interest in the resulting information; or

nation's international reputation, as in the Pentagon Papers case, but rather the more focused and tangible harm of universal nuclear disaster. *The Progressive's* contention that no prior restraint should issue "regardless of the gravity of the injury that might [otherwise] result, unless the government could prove that the threatened harm is virtually certain to occur, would truly render the Constitution a global suicide pact.

Tribe & Remes, *supra* note 2, at 24 (emphasis in original). See also Ferguson, *supra* note 10, at 661 n.83.

¹⁵¹ See, e.g., *Snepp v. United States*, 447 U.S. 507 (1980) (per curiam); *Cole v. Richardson*, 405 U.S. 676 (1972).

¹⁵² 444 U.S. 507 (1980) (per curiam).

¹⁵³ *Id.* at 508.

¹⁵⁴ *Id.* at 509 n.3.

¹⁵⁵ *Id.*

the researcher, by accepting the public financing, accepts restrictions that might otherwise violate the first amendment.¹⁵⁶

A very different situation would be presented, however, if the state imposed sanctions on a publisher who had received confidential government information from another party. In *Landmark Communications, Inc. v. Virginia*,¹⁵⁷ a unanimous Court reversed the conviction of a newspaper publisher who had reported the status of a confidential proceeding before a judicial disciplinary board. In so doing, the Court reaffirmed a principle that has surfaced repeatedly in its recent interpretations of the first amendment: the publication of legitimate news would be impermissibly "chilled" if a newspaper were obliged to decide at its peril whether any of the information that has come into its possession is defamatory, confidential, or illegally transmitted.¹⁵⁸ Accordingly, a publisher in receipt of secret material from a government employee stands on at least an equal constitutional footing with the individual who seeks to disseminate privately generated information.

B. A Framework for Analysis

Having established these general principles, it is now possible to undertake a more detailed consideration of the constitutionality of state-imposed restrictions on scientific speech. There are two general types of concerns that could prompt the state to impose restrictions on scientific communication: the underlying information may conflict with prevailing values or it may be subject to dangerous or unwanted uses.

¹⁵⁶ Cf. *Buckley v. Valeo*, 424 U.S. 1, 51-59, 95 (1976) (per curiam) ("acceptance of public financing entails voluntary acceptance of an expenditure ceiling" otherwise unconstitutional).

¹⁵⁷ 435 U.S. 829 (1978).

¹⁵⁸ See, e.g., *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97 (1979); *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539 (1976); *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469 (1975); *New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam); *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). See also *Cox*, *supra* note 146, at 12.

An exception to the above principle might well be made for instances in which the publisher has knowingly and actively induced a government employee's breach of confidence. See *Cox*, *supra* note 146, at 11-12.

The first rationale strikes a familiar historical chord, for it calls to mind the two most celebrated attempts to impose restrictions on the scientific endeavor: the trial and conviction of Galileo by the Inquisition in Rome, and the Soviet Union's adoption of Lysenko's flawed genetic theories to the exclusion of all alternatives. Along with a Western liberal tradition that affirms the value of intellectual freedom, these ill-fated efforts have done much to discredit the notion that ideas can be inherently harmful. But even today, there are times when scientific theories encounter social resistance because they conflict with accepted views or received tradition. For example, the emerging discipline of human behavioral genetics (so-called "sociobiology") has been criticized in recent years on the grounds that it threatens to undermine the social commitment to democratic and egalitarian values.¹⁵⁹

Suppose, then, that the state enacted a statute imposing criminal sanctions on the dissemination of a specific body of scientific data or ideas that conflicted with majoritarian values. To save the statute from a constitutional challenge, the state would have to show that it had a "compelling" interest in selecting the underlying message or idea for unfavorable treatment. The Supreme Court, however, has not been receptive to regulatory interests that are based on the public's distaste for particular messages or views. Indeed, in what is perhaps the closest precedent, cases dealing with so-called "offensive speech," the Court has declared that the first amendment "strictly limits" the power of government to "shield the public from some kinds of speech on the ground that they are more offensive than others."¹⁶⁰ Thus, in *Cohen v. California*¹⁶¹ the Court rejected the notion that the "States, acting as guardians of public morality, may properly remove [an] offensive word from the public vocabulary."¹⁶² This holding was based on a key principle of first amendment theory, and one that is especially applicable to scientific speech: the "government has no power to restrict expression because of its message, its ideas, its subject matter or its

¹⁵⁹ See, e.g., Wilson, *The Attempt to Suppress Human Behavioral Genetics*, J. GEN. EDUC., Winter 1978, at 277.

¹⁶⁰ *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 209 (1975). See *Eaton v. City of Tulsa*, 415 U.S. 697 (1974); *Brown v. Oklahoma*, 408 U.S. 914 (1972); *Gooding v. Wilson*, 405 U.S. 518 (1972).

¹⁶¹ 403 U.S. 15 (1971).

¹⁶² *Id.* at 22-23.

content.”¹⁶³ Accordingly, unless the Court were to abandon this well-settled principle, it would hold unconstitutional any regulatory measure based on the first rationale.

The government's position would be stronger, however, if it sought to impose restrictions on a specific body of scientific speech that is subject to dangerous or unwanted uses. There are three basic types of technological data that present such hazards: data with applications that are ethically objectionable; data with applications that threaten to produce a social dislocation; and data with applications that implicate national security interests.¹⁶⁴

In the case of the first two types of information, the state could usually achieve its ends by regulating the ways in which the information is used. For example, the ethical concerns arising from the prospect of human cloning could be effectively answered by a statute defining specific applications of the technological data as a criminal offense. By the same token, the state could often avert a disruptive or unwanted social change by restricting the use of any technological information that threatened to produce such a change.¹⁶⁵ In these cases, therefore, the government would have a “less restrictive alternative” to restraints on scientific speech.

Such an alternative would not be available, however, in the case of “national security” data.¹⁶⁶ By definition, the perceived danger in such a setting is posed by hostile nations or terrorist groups who would

¹⁶³ *Police Dep't of Chicago v. Mosley*, 408 U.S. 92, 95 (1972). See also *Consolidated Edison Co. v. Public Serv. Comm'n*, 447 U.S. 530 (1980); *Carey v. Brown*, 447 U.S. 455 (1980). See generally J. ELY, *supra* note 16, at 111-16; L. TRIBE, *supra* note 16, § 12-2; Karst, *Equality as a Central Principle of the First Amendment*, 43 U. CHI. L. REV. 20 (1975).

¹⁶⁴ See text accompanying notes 21-36 *supra*.

¹⁶⁵ It should be noted, however, that the government might face insurmountable difficulties in attempting to regulate the use of a much-sought-after technology in a free society. This would probably hold true, for example, in the case of a life-extending technology. If the government could not achieve its ends through the regulation of use, the constitutionality of criminal restrictions on the dissemination of the data would turn on the gravity of the “evil”—that is, the nature and magnitude of the threatened social dislocation—and the likelihood of its occurrence. See text accompanying notes 138-40 *supra*.

¹⁶⁶ The following discussion does not pertain to data subject only to military use, which may merely be afforded limited protection. See text accompanying note 124 *supra*.

not be deterred by, or even subject to, criminal prosecution. Predictably, therefore, in dealing with the threatened dissemination of information having national security overtones, the government would attempt to obtain a prior restraint on publication.

To do so successfully, the state would first be required to show that the information is indeed subject to the claimed dangerous use and that the basic data is not already in the public domain.¹⁶⁷ If such a showing could be made, the state would then be required to demonstrate that the threatened harm is sufficiently weighty to justify a prior restraint. As a general matter, the Supreme Court has acknowledged that "no governmental interest is more compelling than the security of the Nation"¹⁶⁸ and that this interest sometimes entails protecting the secrecy of certain kinds of information.¹⁶⁹ However, on the facts of a given case, the Court would necessarily look to the gravity of the specific "evil" that the state is seeking to avert and the likelihood of its occurrence.

Turning first to the "likelihood of occurrence," the crucial inquiry would address the probability that publication of the information at issue will result in the asserted harm. More specifically, the analysis would consider the likelihood that the information will be used by a third party to develop the relevant capability as a direct

¹⁶⁷ In this regard, the report of the House Committee on Government Operations on the government's classification of private ideas is instructive:

Whether or not a piece of information has entered the public domain has been a matter for case-by-case adjudication—the subject apparently not lending itself to the imposition of general rules when potentially dangerous national security information is at issue. The few cases specifically on point suggest that while official publication will likely place the information in the public domain, anything short of that will not unless public knowledge is so pervasive as to render classification meaningless. And public awareness of parts of the whole will not necessarily be interpreted as public knowledge of an assemblage of those parts. The issue is perhaps more conducive to judicial resolution when the data involved has undergone an orderly classification process. Under the atomic energy statutes however, as illustrated in *Progressive*, the "born classified" concept allows that step to be omitted and leaves only the subject matter itself for review.

HOUSE REPORT, *supra* note 5, at 159.

¹⁶⁸ *Haig v. Agee*, 101 S. Ct. 2766, 2782 (1981).

¹⁶⁹ *See id.*

result of publication.¹⁷⁰ This issue is especially important because the transfer of technical data, with no subsequent interaction between those disseminating the information and those receiving it, is a relatively ineffective method of transferring technology.¹⁷¹

In coming to terms with the issue, two lines of inquiry would be particularly relevant. First, does the effective use of the information require a large industrial capability or sophisticated technological resources? If not, the government could show a high "likelihood of occurrence" simply because the data would be subject to use by an unlimited number of third parties, including terrorist groups and perhaps even individuals. Second, is the information known to be in the possession of nations that pose a potential military threat to the United States? If not, and if the data confers a strategic advantage on the United States, the government could show that the information would almost certainly be used by rival nations to develop an equivalent capability or effective countermeasure.¹⁷²

By way of contrast, assume that the use of the data required some degree of technological sophistication and that the class of potential users was therefore limited. Assume further that the nations posing a recognized military threat to the United States were known to possess the capability or its functional equivalent. In such a case,¹⁷³ the countries that did not have the data, but did possess the requisite technological resources, might well be restrained from using the information by political, economic, or diplomatic considerations. It is conceivable, of

¹⁷⁰ The text is referring here to the utilization of the data to develop the relevant capability, and not to the subsequent utilization of the capability against the nation. It seems clear that a harm to the national security would follow from the mere acquisition of new military capabilities by hostile nations or groups.

¹⁷¹ EXPORT ADMINISTRATION, U.S. DEP'T OF COMMERCE, 116TH REPORT ON U.S. EXPORT CONTROLS, App. D, at 128 (April-September 1977).

¹⁷² This discussion assumes, of course, that a strategic advantage would promote the national security of the United States.

¹⁷³ This was essentially the factual situation presented in *United States v. The Progressive, Inc.*, 467 F. Supp. 990, 994 (W.D. Wis.), *appeal dismissed*, 610 F.2d 819 (7th Cir. 1979). As the district court noted, "[A] *sine qua non* to thermonuclear capability is a large, sophisticated industrial capability coupled with a coterie of imaginative, resourceful scientists and technicians." *Id.* at 993. Furthermore, at the time of the decision, five nations were known to possess the hydrogen bomb, namely France, England, China, the Soviet Union, and the United States.

course, that one such nation would use the data, either immediately or at some later date. It is also conceivable that other countries or groups would subsequently acquire the needed technological resources and put the information to use. But these possibilities would necessarily be speculative. Accordingly, in a case such as this, the government could establish nothing more than a "reasonable possibility" that the publication of the data would result in the asserted harm.

Turning to the "gravity of the danger," the relevant inquiry would address both the nature and the magnitude of the harm that would result if the information at issue were indeed used by a third party. By relying on these two factors, the various forms of technological data implicating national security interests can be ranked in a hierarchy based on the danger posed by third party acquisition of the particular capability.

The most serious danger would arise from information that could be used to acquire a destructive capability exposing large populations to a threat of death or physical harm. This category would include technological data that either directly confers a vast destructive power or enables such a power to be used. For example, on the latter point, some observers have cited the imminent development of "portable" nuclear weapons that could fit in a suitcase or small trunk and thus render unnecessary a sophisticated delivery system.¹⁷⁴ In a similar vein, critics of the current research on "isotope separation" have claimed that this technology could provide a source of nuclear weapons fuel to third parties who would otherwise be precluded from deploying such weapons by a lack of scarce plutonium.¹⁷⁵

A slightly different danger would arise from information with uses that could alter the military balance between the United States and the Soviet Union, two nations that already possess enormous destructive powers. While the potential harm in this case is perhaps less easily grasped than that in the first category, it is nevertheless substantial. Suppose, for instance, that a major advance in particle beam technology conferred a strategic advantage on the United States.¹⁷⁶

¹⁷⁴ Etheredge, *The Old Imagery of War Is Outdated*, N.Y. Times, May 27, 1981, § A, at 27, col. 3.

¹⁷⁵ See, e.g., Sinsheimer, *The Presumptions of Science*, *supra* note 30, at 23.

¹⁷⁶ Although some analysts have questioned the feasibility of particle beam weapons, see, e.g., Parmentola & Tsipis, *Particle Beam Technology*, SCIENTIFIC AM.,

Such an advantage would make the prospect of a Soviet strike more remote and could also be translated into a foreign policy that more effectively secured national interests threatened by Soviet actions. Consequently, if the relevant information fell into Soviet hands, the gains to the security of the nation could be wholly lost, and the ability to safeguard national interests correspondingly impaired.

Beyond these possibilities, there are other forms of technological data that might pose lesser dangers to national security in either of two ways: by providing the technology to develop or upgrade the military equipment of a potential adversary, or by providing insights into the military capabilities of the United States that could facilitate the development of countermeasures.¹⁷⁷ In addition, the transfer of some types of technological information could have foreign policy implications that bear on national security concerns. As the Supreme Court has recognized, the “[p]rotection of the foreign policy of the United States is a governmental interest of great importance, since foreign policy and national security considerations cannot neatly be compartmentalized.”¹⁷⁸ Accordingly, the government might seek to prevent the transfer of information that could enhance another country’s capabilities in a manner inconsistent with the United States’ foreign policy goals, for example, by improving the ability of one nation to threaten a neighboring country that is aligned with the United States.⁷⁹

If the government could show in a given case something more than a “reasonable possibility” of occurrence, the relative position of the threatened danger on this kind of hierarchy would determine the outcome of the first amendment challenge to the prior restraint. In fact, if the state could show that occurrence was likely, its actions would probably be upheld as long as the information was genuinely “important to national security.”¹⁸⁰ On the other hand, if there was only a “reasonable possibility” of occurrence, the restraint on publica-

April 1979, at 54, there is mounting evidence that both the United States and the Soviet Union are pursuing the development of such capabilities. See *N.Y. Times*, Feb. 10, 1980, at 1, col. 4.

¹⁷⁷ EXPORT ADMINISTRATION, U.S. DEP’T OF COMMERCE, *supra* note 171, at 130.

¹⁷⁸ *Haig v. Agee*, 101 S. Ct. 2766, 2782 (1981).

¹⁷⁹ HOUSE REPORT, *supra* note 5, at 101.

¹⁸⁰ *Snepp v. United States*, 447 U.S. 507, 509 n.3 (1980) (*per curiam*).

tion would not be sustained unless the threatened danger was sufficiently grave to rank near the top of the hierarchy.

VI. On The Futility of Policing Ideas

This Article has proceeded on the assumption that the government could preserve a scientific or technological "secret" if it were constitutionally permitted to do so. There is, however, good reason to doubt that such a secret could be maintained for an extended period of time. Even if restraints were imposed on the domestic publication of a particular body of information, scientists in other countries would remain free to pursue the same avenue of investigation that produced the information. This is a particularly important point because, as noted earlier, scientific advances usually build upon a foundation of knowledge that is shared by all professionals in the relevant field.¹⁸¹ Thus, a major scientific or technological advance would usually be duplicated by other advanced nations within a period of years, if not sooner.¹⁸²

It is quite possible, of course, that the maintenance of such a "lead time" could be highly significant when national security interests are at stake.¹⁸³ But the preservation of a scientific secret for even a short period of time would be very difficult.¹⁸⁴ Indeed, given the net-

¹⁸¹ See text accompanying notes 104-05 *supra*.

¹⁸² See Cheh, *supra* note 2, at 204 n.268.

¹⁸³ Note, *Developments in the Law—The National Security Interest and Civil Liberties*, 85 HARV. L. REV. 1130, 1190 (1972). This point was clearly demonstrated during World War II, when Allied scientists worked to complete the development of a nuclear weapon before Nazi Germany achieved the same end. See C. SNOW, *THE PHYSICISTS* 104-05 (1981).

¹⁸⁴ The government's task would be considerably lessened, of course, if the information were in its exclusive possession. A House subcommittee that recently investigated the disclosure of information on the so-called Stealth aircraft concluded that the "Pentagon must totally disabuse itself of the philosophy . . . that in a democracy there is nothing the Department can do to prevent security leaks, or track them down when they occur." HOUSE COMM. ON ARMED SERVICES, *LEAKS OF CLASSIFIED NATIONAL DEFENSE INFORMATION—STEALTH AIRCRAFT*, H.R. DOC. NO. 30, 96th Cong., 2d Sess. 9 (1981). The subcommittee recommended legislation that would require that "any publication of [national security] information by the media be accompanied by the name of the source of such information." *Id.*

work of informal communications that exists within the scientific community,¹⁸⁵ the state would have to monitor virtually every domestic publication to ensure that the information would not be disclosed publicly. This point was clearly illustrated by the outcome of the *Progressive* litigation. After the district court enjoined the magazine from publishing the hydrogen bomb data, the government was forced to apply for a second injunction when a California newspaper acquired the same information.¹⁸⁶ This effort also proved futile, however, for yet another newspaper published the basic data before the government was able to institute any actions against the publisher.¹⁸⁷

One possible solution to such an exercise in futility is illustrated by an agreement that the National Security Agency has reached with computer scientists doing cryptographic research.¹⁸⁸ Under the agreement, the research scientists consented to submit the results of their work to the NSA for prepublication review in order to reduce the possibility that a foreign government might gain a military advantage from a newly developed code.¹⁸⁹ By relying on the voluntary cooperation of scientists, such an arrangement clearly charges the scientific establishment with the social responsibilities of a public trustee or fiduciary. But the imposition of such obligations may be entirely appropriate, given the far-reaching implications that the scientific endeavor now carries for the public.

If the scientific community were to accept the duties of a public trustee—and there is evidence suggesting that it has already done so¹⁹⁰—a system of self-regulation could be explored routinely as a first step in resolving conflicts between the government's regulatory inter-

¹⁸⁵ Although the most important form of scientific communication is the publication of papers in professional journals, scientists also rely heavily on informal exchanges with colleagues who work in the same research tradition. G. KNELLER, *supra* note 11, at 195-98.

¹⁸⁶ See Cheh, *supra* note 2, at 166 n.15; N.Y. Times, Sept. 18, 1979, § A, at 1, col. 6.

¹⁸⁷ N.Y. Times, Sept. 18, 1979, § A, at 1, col. 6.

¹⁸⁸ *Id.*, Feb. 15, 1981, § E, at 20, col. 2.

¹⁸⁹ *Id.*

¹⁹⁰ Perhaps most notably, at the Asilomar Conference in February 1975 an international conclave of molecular biologists declared a moratorium on recombinant DNA research until the potential risks could be more fully assessed. C. GROBSTEIN, *supra* note 28, at 2, 23-35.

ests and scientific freedom. Such an approach would commit the initial assessment of the government's concerns to the informed but critical judgment of the affected researchers. If the scientists are persuaded by the government's claims, the resulting self-regulation would provide the surest guarantee against public disclosure.

On the other hand, if the two sides are unable to reach an agreement, the conflict will be resolved in the courts. Importantly, however, an adjudication of the issue will not require a sharp break from traditional first amendment doctrine. On the contrary, the application of standard first amendment principles will generally provide a satisfactory basis for deciding the novel constitutional issues that will arise from governmental attempts to regulate certain forms of scientific and technological information. And this conclusion is perhaps the highest tribute to the enduring ability of those principles to accommodate the claims of free speech with the legitimate interests of the public welfare.

6123 USC
CRS MAIN FILE COPY

What price security?

S-83 02496

A National Academy panel evaluates trade-offs between dangers to national security that arise from technology transfers and threats to the openness of scientific communication that are caused by too much secrecy.

DeLo Corson

"There is an overlap between technological information and national security which inevitably produces tension. This tension results from the scientist's desire for unconstrained research and publication on the one hand, and the Federal government's need to protect certain information from potential foreign adversaries who might use that information against this nation. Both are powerful forces. Thus, it should not be a surprise that finding a workable and just balance between them is quite difficult." So said Admiral Bobby R. Inman, then Deputy Director of the Central Intelligence Agency, in a speech at the 7 January 1982 meeting of the American Association for the Advancement of Science.

DeLo Corson, a physicist and former president of Cornell University, led the National Academy panel.

Inman's speech has since sparked widespread discussions aimed at delineating the differing needs of these two forces and suggesting ways to balance them. In fact, the tension about which Inman spoke, and the dilemma it poses, were the focus for a study recently completed under my chairmanship, entitled "Scientific Communication and National Security" (PHYSICS TODAY, November, page 69). The study, conducted under the auspices of the National Academies of Science and Engineering, considered the interests of both national security and scientific communication; attention focused on the control mechanisms now being used to restrict the flow of information and on the application of these controls; the committee also recommended specific improvements to the system.

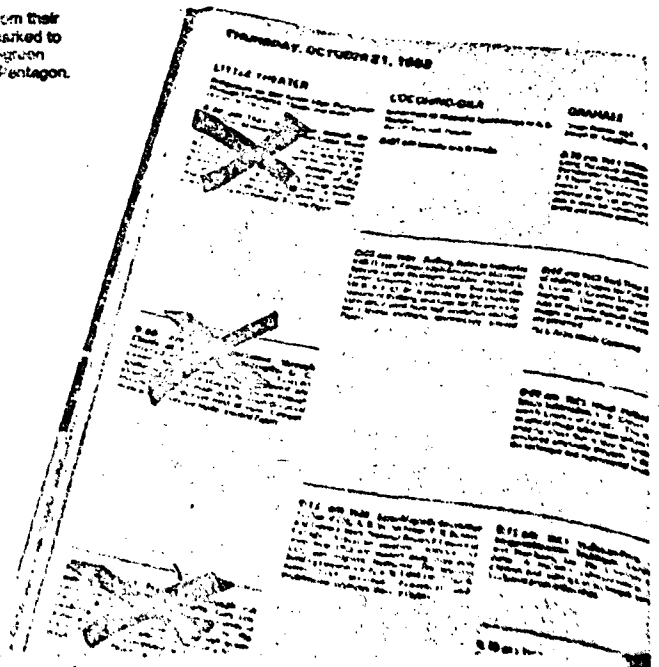
The underlying conflict between the drive for security and the drive to open

communication is not a new issue. Recently, however, concerns about national security as well as concerns about the free flow of information among scientists have increased. Why?

Recent events increase concerns

Although administrative concern over the technology-transfer problem increased during the last Administration, it has escalated sharply in the current one. This new sense of alarm has emerged, to some degree at least, from a change in perceptions. The US intelligence community, in fact, has identified four trends as significant. ▶ The US lead in at least some areas of military technology has diminished. The intelligence community sees this diminishing lead as a result of Soviet absorption of Western technology. ▶ Military systems are depending more and more on such high technol-

Optical Society program (right) from their November meeting in Tucson, is marked to indicate the invited papers on blue-green lasers that were withdrawn by the Pentagon.



PHYSICS TODAY / FEBRUARY 1983
P 42-9547
V-36

ogies as state-of-the-art microelectronics, lasers and so forth.

► A steadily increasing share of these technologies has both military and non-military applications; there is substantial difficulty in controlling leaks in non-military systems.

► Recent American foreign policy has multiplied the number of routes for leakage. Significant expansion of East-West trade in the 1970s, for example, has resulted in a variety of agreements that further encourage the transfer of technology.

Adding further to the alarm is a concerted effort at the Soviet Union is making a concerted effort to acquire scientific and technical information. This view was expressed strongly by Lawrence J. Brady, Assistant Secretary of Commerce, in a speech before the intelligence community last March. He said:

Operating out of embassies, consulates, and so-called "business delegations," KGB operatives have blanketed the developed capitalist countries with a network that operates like a gigantic vacuum cleaner, sucking up formulas, patents, blueprints and know-how with frightening precision. We believe these operations rank higher in priority even than the collection of military intelligence. . . This network seeks to exploit the "soft underbelly"—the individuals who, out of idealism or greed, fall victim to intelligence schemes;

our traditions of an open press and unrestricted access to knowledge; and finally, the desire of academia to jealously preserve its prerogatives as a community of scholars unencumbered by government regulation. Certainly, these freedoms provide the underpinning of the American way of life. It is time, however, to ask what price we must pay if we are unable to protect our secrets?

The question of what price the Administration is willing to pay to keep information out of the hands of adversaries, particularly the Soviet Union, is perhaps the central concern of the scientific community. And now this concern has been heightened, primarily because of recent events and what they imply regarding further restrictions on scientific communication.

Notable among these events have been efforts to elicit the cooperation of universities in restricting the movements of visiting Soviet scientists. In addition, there have been repeated instances in which the Pentagon or the Department of State has sought to prevent scheduled papers from being presented at scientific conferences. One such incident that recently received wide publicity took place at the Society of Photo-optical Instrumentation Engineers' conference in San Diego in August. The Pentagon had nearly 150 papers withdrawn several days before the meeting. It now appears that many of these papers will, after all, receive clearance and be included in the published proceedings from this meeting. Similar incidents in which scheduled papers have been withdrawn from scientific meetings have taken place before and apparently will continue to take place, as the Optical Society of America discovered in November when several papers were withdrawn from its meeting in Tucson. These events stem, in part, from a confusion over how to apply the Federal regulations to the scientific and academic community.

Panel studies key issues:

Our panel of 19 people included a former Under Secretary of Defense, a former Under Secretary of Energy, a former Director of the National Science Foundation, a former Presidential Science Advisor, four former members of the President's Science Advisory Committee, five members or former members of the National Science Board, six current or former university presidents, one former Director of the National Security Agency, four execu-

tives of high-technology industry, several present or former members of the Defense Science Board and two lawyers.

Our charge included four tasks:

- An examination of national-security issues and scientific communication interests within the context of certain fields of science and technology
- A review of the controls used in restricting scientific communication as well as identification of the issues arising from the use of the controls
- A rigorous evaluation of the critical issues concerning the application of controls, and
- The development of ways to make the system operate more effectively.

Although the panel's mission was to investigate the effects of restrictions on scientific communication in general, it found in reaching its recommendations that the university requires separate consideration within the context of the US research community. Restrictions on open communication have categorically different implications for universities than they do for industrial, governmental and other realms of the community; there are two main reasons for this distinction:

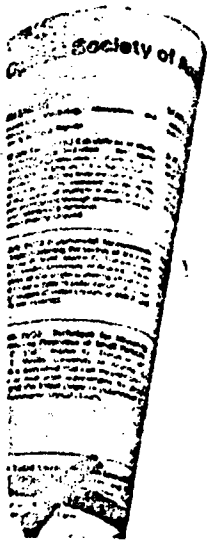
- Universities integrate research and education; thus, any adverse effects on research will also adversely affect the quality of education for the next generation of scientists and engineers.
- Unlike other research institutions, universities have never established broad controls on access to information to ensure that sensitive information be protected. Such restrictions, therefore, would present an unfamiliar and unwelcome challenge to the university.

Because the potential national security concerns are most likely to arise in work that is funded by the government, the panel's conclusions concentrate on government-supported research.

While much of our report applies to basic industrial research just as much as it applies to university research, there are important questions bearing on industry that we have not addressed at all. For example, how does one treat the problem of communication with a multinational company that has laboratories abroad and foreign subsidiaries? For many, this may be the most important question of all; I regret I cannot help, for this question requires study by a new group constituted in a different way.

Due to both the current level of concern and the panel's limited time and resources, study focused on technology transfer to the USSR from the US.

To study these issues, the panel had



nature of the technology-leakage problem was. We realized early on that we would have to operate on a classified basis; consequently we arranged for security clearance for all panel members at the secret level. In addition, six of our members, who held security clearances at the highest level, arranged for intelligence briefings and discussions at the very highest security levels and reported back to the full panel at the secret level. They also produced a Secret report which is on file in the National Academy of Sciences. In addition, they produced an unclassified report, which is included in our panel report as an appendix, and which gives a clear picture of the technology-leakage problem.

The panel is unanimous in its conclusions and recommendations.

Major suggestions and conclusions

The evidence from all sources suggests that indeed there is a substantial and serious technology-transfer problem. There is a continuing flow of products, processes and ideas from the US and its allies to the Soviet Union, through both overt and covert means. Although much of this unwanted transfer has mattered little to US security, either because the US did not enjoy a monopoly on a particular technology or because the technology in question had little or no military significance, a substantial portion of the transfer has been damaging to national security (See the table for some evidence presented by the Central Intelligence Agency). These damaging transfers have taken place through the legal as well as illegal sale of products, through transfers via third countries and through a highly organized espionage operation.

Although a good deal of information has been transferred through open scientific communication, the panel concludes that, in comparison with other channels of technology transfer, open scientific communication involving the research community does not threaten our near-term military position. Given both this conclusion and our concern for finding an approach that will maintain the vitality of our universities and their roles in education and research, while at the same time protecting the security of our advanced technology, how should we proceed?

The panel believes that scientific research and technological development are best nurtured in an environment where such efforts are dispersed but interdependent. Openness and a free flow of information are essential aspects of such an environment. The technological leadership that the US enjoys is based in no small part on a

turn depends on effective communication among scientists, and between scientists and engineers; the short-term security achieved by restricting the flow of information is purchased at a price.

After weighing the alternatives, the panel concludes that the best way to ensure long-term national security lies in a strategy of "security by accomplishment," and that an essential ingredient of technological accomplishment is open and free scientific communication. Such a policy involves risk, because new scientific findings will inevitably be conveyed to US adversaries. Nonetheless, the panel believes the risk is acceptable because American industrial and military institutions are able to develop new technology swiftly enough to give the US a continuing advantage over its military adversaries.

Against this general background, the panel comes to three specific conclusions:

- The vast majority of university research programs, whether basic or applied, should be subject to no limitations on access or communications.
- Where specific information has direct military relevance and must perforce be kept secret, it should be classified strictly and guarded carefully.

classified research projects, or to establish off-campus classified facilities, is a matter to be decided by individual universities.

► There are a few gray areas of research that are sensitive from a security standpoint, but where classification is not appropriate. These areas are at the ill-defined boundary between applications and basic research and are characteristic of fields where the time from discovery to application is short. (At present, a portion of the field of microelectronics is the most visible of these technologies.)

While it is impossible to specify these gray areas with precision, there are some broad criteria that help to define the few areas in question. The panel recommends that no restrictions of any kind that limit access or communication should be applied to any area of university research, basic or applied, unless it involves technology meeting all of the following four criteria:

- The technology is developing rapidly and the time from basic science to application is short; and
- The technology has identifiable direct military applications, or is dual-use, and involves process- or production-related techniques; and
- Transfer of the technology would give the USSR a significant near-term

Acquisitions from the West affecting Soviet military technology

Key technology area	Notable successes
Computers	Purchases and acquisitions of complete systems designs, concepts, hardware and software, including a wide variety of Western general purpose computers and minicomputers, for military applications.
Microelectronics	Complete industrial processes and semiconductor manufacturing equipment capable of meeting all Soviet military requirements. If acquirers were combined.
Signal Processing	Acquisitions of processing equipment and know-how.
Manufacturing	Acquisitions of automated and precision manufacturing equipment for electronics, materials, and optical and laser weapons technology; acquisition of information on manufacturing technology related to weapons, ammunition, and aircraft parts including turbine blades, computers, and electronic components; acquisition of machine tools for cutting large gears for ship propulsion systems.
Communications	Acquisition of low-power, low-noise, high-sensitivity receivers.
Lasers	Acquisition of optical, pulsed power sources, and other laser-related components, including special optical stores and mirror technology suitable for future laser weapons.
Guidance and Navigation	Acquisitions of marine and other navigation receivers, advanced inertial-guidance components, including mirrors and laser gyro; acquisitions of missile guidance subsystems; acquisitions of precision machinery for ball-bearing production for missile and other applications; acquisition of missile test-range instrumentation systems and documentation and precision classification for collecting data critical to postflight ball-to-missile analysis.
Structural Materials	Purchases and acquisitions of Western titanium alloys, welding equipment, and furnaces for producing titanium plate of large size applicable to submarine construction.
Propulsion	Missile technology; some ground-propulsion technology (turbine, turbines, and rockets); purchases and acquisitions of advanced jet-engine fabrication technology and jet-engine design information.
Acoustical Sensors	Acquisitions of underwater navigation and direction-finding equipment.
Electro-optical Sensors	Acquisition of information on satellite technology, laser range finders, and underwater low-light-level television cameras and systems for remote operation.
Radars	Acquisitions and exploitations of air defense radars and engine designs for missile systems.

Life adapted from a Central Intelligence Agency report entitled "Soviet Acquisition of Western Technology," April 1982.

military advantage; and

► Either the US is the only source of information about the technology, or other friendly nations that could also be the source have control systems at least as secure as ours.

The panel recommends that in the limited number of instances in which all of the above criteria are met, but where classification is unwarranted, the values of open science can be preserved and the needs of government can be met by written agreements or contracts no more restrictive than the following:

► Prohibition of direct participation in government-supported research projects by nationals of designated foreign countries but with no attempt to limit physical access to university space or facilities or to limit enrollment in any classroom course or study. The danger to national security lies in the immersion of a suspect visitor in a research program over an extended period, not in casual observation of equipment or research data.

► Submission of stipulated manuscripts simultaneously to the publisher and to the Federal agency contract officer, with the contract officer having 60 days to seek modifications in the manuscript if he so wishes.

The review period is not intended to give the government the power to order changes. The right and freedom to publish remain with the university as they do with all unclassified research. The government nonetheless is a powerful negotiator in these discussions; it has the ultimate power to classify the research or to cancel the contract.

Knottier problems

The panel recognized the difficulty of limiting the access of foreign visitors on campuses to sensitive information, particularly when universities typically have people who are not working on federally-funded projects but who have free access to the laboratories and all that goes on within the university.

Let me simplify the problem by suggesting what might happen in a specific case. Visitors come to universities with restrictions on their visas. Such restrictions may include travel restrictions, restrictions on what they can work on, and currently there might also be restrictions on what they can see. The contract officer occasionally checks up on the visitor and he also asks the university to report on what these particular visitors are up to. Certainly, according to our recommendations, the university would be alerted to the problem and notified that the visitors should not be supported with project funds over an extended period of time.

In the case of the similar research laboratory next door, performing non-

government-funded research, we suggested that it would not be inappropriate for the university to respond affirmatively to requests from government agencies for information about possible attempts by the visitors to gain support to work with the nongovernment-funded project over an extended period. We reasoned that if the researchers did obtain that type of support, in doing so they would be presumably violating the terms of their visa. Thus we think it's appropriate for the university to respond affirmatively if asked, when those visa restrictions are being violated. Such requests, however, should not require surveillance or monitoring of foreign nationals by the universities.

It is important for the welfare of the country that universities' educational and research programs remain vital. The procedures recommended by the panel for dealing with the gray areas of research are intended to protect university interests, and at the same time to be responsive to the government's requirements.

The panel believes that the provisions of Export Administration Regulations and International Traffic in Arms Regulations should not be invoked to deal with these gray areas in government-funded university research. Rather, the appropriate procedure should be incorporated in research contracts or other written agreements in those rare cases where some measure of control is required. Furthermore, the panel believes that universities and industrial research laboratories should be treated in exactly the same way insofar as EAR and ITAR are concerned.

Writing the contract ahead of time poses two problems. The first is that one never knows what is going to happen; perhaps something will come up that was not anticipated in the contract. The second is that Federal contracting officers may act overcautiously in protecting themselves by writing in restrictions that are unnecessary. Both are real concerns. To address the first problem—not knowing what's going to come up—we'd like to have the rules clearly understood ahead of time, insofar as they can be, so that everybody knows what the rules are and can play by the same rules. When cases come up where it is necessary to elaborate, we believe that constructive discussion can take place and problems can usually be resolved if there exists an atmosphere of good communication.

As an example of such a resolution, I can cite the situation that began several years ago in the field of cryptography. There were several instances; one in particular occurred in about 1978. A young researcher at the University of

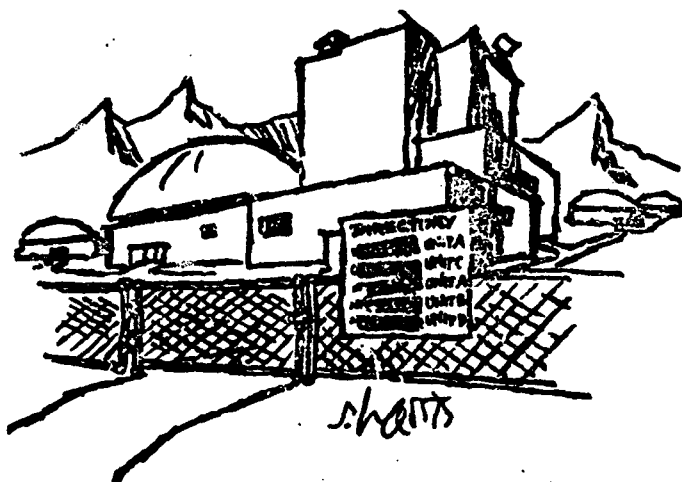
Wisconsin in Milwaukee applied for a patent on a cryptographic invention he had made. He didn't hear from the Patent Office for a long time. Eventually he received a post card as the only response to the application—a post card saying that his research program had been classified Secret and that he was not to talk to anybody about it. This action was authorized under the Invention Secrecy Act.

Admiral Inman played a major role in resolving that issue and reducing a tense situation to one that is now handled on a voluntary basis. The American Council on Education also played a lead role by convening a study group on the cryptography problem, in which the mathematicians participated. I also participated in the very first discussion of that problem at the American Council on Education, where I first met Inman. As a result of these discussions, people working in cryptography now submit their papers to the National Security Agency for comment; simultaneously they submit their papers to the publisher. Some 50 papers have been submitted under this voluntary arrangement. I think changes or suggested changes have been proposed by NSA in a couple of cases, but I have not heard of any great dissatisfaction. I also believe that there are some people working in the field who have declined to cooperate and are going ahead on their own. We spoke both with the National Security people and with people from universities with researchers in the field, and all of them expressed satisfaction with the current system. This is an example of what can happen when people get together and talk about the problem.

The panel believes, however, that one cannot extend this particular system to other research. Cryptography is a very narrow field in which everybody working in it knows everybody else working in it, and the focus of the research is limited and generally well-defined. This is not true for most other fields of research.

The second problem—the overcautious contract officer writing in unnecessary restrictions—is harder to deal with. I suspect that this problem is part of what happened at the San Diego SPIE Conference in August. In that instance, however, it wasn't the contract officer who was overcautious, but rather it was somebody in the Pentagon; I don't know how to protect against Pentagon intervention.

The Defense Department supports a significant amount of first-rate basic research, their so-called G.1 research. Traditionally, research supported by G.1 funding is unclassified, unrestricted, and free for publication. I suspect that now there is a move to restrict G.1 supported research in various ways,



and there are many contract officers who are writing individual contracts for this research. Consider, for example, a situation in which somebody in the S.I. office in the Defense Advanced Research Project Agency decides to support a certain program but he personally doesn't write the contract. Somebody at Wright-Patterson Air Development Center writes the contract. The person who writes the contract is eager not to get in any trouble, so he writes restrictions in. I don't know how to deal with that problem, except by starting at the highest level, setting major policy issues and establishing educational programs for contract officers. I am glad that the Office of Science and Technology Policy is now interested in this kind of problem.

Although these are major problems, and we recognize them, the panel felt that if we could write the agreements ahead of time, so that everybody knew the rules, we would have gained something.

The panel has studied the control system now in effect, and the report has some substantial discussion of the system and its problems. The panel's suggestions apply equally to industrial and university research. The current system is undergoing rapid change. Because the perceived nature of the technology leak problem has shifted only recently, government control mechanisms themselves are still being adjusted to meet the new perceptions.

In a fundamental sense, government is still in the early stages of the learning process as it reorients existing laws, policies and programs—designed for other purposes—to achieve a new objective, the dimensions of which are not yet fully determined. The adjustment is particularly difficult because the current effort to understand and control unwanted technology transfer is unavoidably fragmented within the

Federal establishment. Four intelligence agencies—the FBI, the CIA, the Defense Intelligence Agency and the National Security Agency—share the job of gathering intelligence on the nature, extent and significance of unwanted transfers.

Major regulatory authority is also split among three separate offices: the Department of Commerce's EAR administrators, the Department of State's ITAR administrators, and the Department of State's Visa Processing Office. These offices depend heavily on outside units in the defense and intelligence communities for advice as they reach their judgments.

Similarly diffuse is the government's authority for classifying information and for monitoring results from the research and development that it funds. Regulatory enforcement shows similar diversity and includes yet another agency, the Department of Treasury's Customs Service. The panel discovered, not surprisingly, that few people inside or outside the government truly understand the government's technology-transfer control effort.

The panel believes that there is much room for improvement in targeting the government's efforts to prevent unwanted technology transfer. Priorities must be set and communicated. The panel believes that the government should concentrate on the most feasible forms of control and should avoid regulations that impose compliance burdens without significantly affecting leakage. The government should concentrate its resources more systematically on those technologies that are of greatest relevance to near-term Soviet military strength.

Finally, the panel addressed problems of inadequate staffing in agencies that deal with control measures, as well as problems of inadequate com-

munication between the research community and the Federal agencies. The panel also identified areas where the research community might help the government assess the nature of the technology-transfer problem more reliably.

In assessing the current policies and procedures, we heard the word "confusion" from just about everybody we spoke to about both the ITAR and EAR.

Let me give you an example of the complexity of the system. In the Export Administration Act of 1979, an act which has been revised regularly and is the underlying legislation for EAR, it was specified that the Commodity Control List should be based on something called the Militarily Critical Technologies List. The Commodity Control List is the basis for licensing exports and the Militarily Critical Technologies List is now undergoing its second revision. The third version of this list is going to be issued some time in the immediate future. The second version was a 700-page book, all of which is classified Secret. If one wants to take this to its logical end, it means that the people who are going to be subject to heavy fines through the implementation of these regulations will not be able to know what it is that the violation is based on. The regulations are administered somewhat more intelligently than this sounds, but nonetheless individual parts of the Commodity Control List are classified individually. For example, some are Confidential, some are Secret and some are Unclassified. Regardless of classification, all are subject to export restrictions determined by EAR. Among the unclassified technologies are such things as high-vacuum technology, or manufacturing techniques for the mass production of ultra-high frequency generators, and techniques for making certain kinds of magnets which industrial people are making every day of the week.

The list has been developed by dedicated people who have taken a military system apart piece by piece to see what went into it; those people have taken their work seriously and they've done an excellent job of finding what underlies every military system that exists.

Due to the comprehensiveness of this list and its classification, however, there seems to be no way to start from that list and arrive at a straightforward and clear definition of what it is that the regulations are going to apply to. Thus one of our recommendations is to streamline the MCTL. Our general suggestion was to build high walls around narrow areas that are clearly defined, with priorities established in words that everybody can understand. I don't have any great hope, however, that tomorrow's mail will bring such a list to my desk. □

16

CRS Main File Copy

JC 660 C

82-

82-2422



When SCIENCE Is Outlawed...

Outlaw scientists may have to turn to a scientific samizdat if the Reagan administration succeeds in clamping new controls on research and publishing in the name of national security. **by John Pike**

DRIFTING OFF THE EASTERN shore of the United States, an innocent-looking buoy bobbed up and down with the waves until a U.S. naval vessel fished it out of the water. Examined closely, the buoy gave up its guilty secret: It was a Soviet antisubmarine device dropped near American waters to monitor ocean temperature and currents. Most disturbing of all was the discovery that the miniaturized electronics in the buoy used tiny integrated circuits based on American designs—evidently stolen and then

copied by the Soviets. "That's a scary achievement," commented one defense official. And indeed no less than Defense Secretary Caspar Weinberger has cited this case as evidence of the Soviets' "massive, systematic effort to get advanced technology from the West . . . to support the Soviet military buildup."

But was it such a "scary achievement?" The integrated circuits found in the buoy were at least three years out of date—and three years in the fast-paced semiconductor industry is time enough for an entirely new generation of devices to appear. Nonetheless, the Reagan administration has exploited this episode and others like it to support a wide-ranging crackdown

on the free flow of scientific information. The crackdown is coming on three fronts: stringent new controls on the Freedom of Information Act, a new executive order authorizing sweeping government censorship, and now a major thrust to stymie the dissemination of scientific knowledge.

The Reagan administration entered its second year with the makings of a return to the scientific McCarthyism of the Oppenheimer inquisition. Several major pronouncements by high-ranking administration officials—amounting to a naked power-grab by the government to shackle the scientific community in the name of national security—have led to protests by academics concerned about the im-

JOHN PIKE writes frequently on science, technology and public policy. He is currently completing a book and a video on the exploration of outer space.

INQUIRY (San Francisco) US March 27, 1982

P 25

minent loss of their First Amendment protections of freedom of speech. At stake in this growing controversy is the ability of scientists to inquire and publish free from the withering, scrutiny of government censors.

The spearhead of this assault on scientific freedom was a speech by

Admiral Bobby Ray Inman, currently deputy director of the CIA, in Washington, D.C., on January 7. Addressing a symposium at the annual meeting of the American Association for the Advancement of Science (AAAS), Inman asserted that the free exchange of ideas among scien-

tists was aiding the Soviet military buildup, and called for a system of voluntary controls—including pre-publication review of technical papers—to restrict the flow of information in such fields as "computer hardware and software, other electronic gear and techniques, lasers, cop pro-

Our Unofficial Secrets Act

by Jonathan Marshall

LONG BEFORE THE Reagan administration made its highly publicized threat to drop a wall of secrecy around the scientific community, another branch of scholars was already feeling the weight of government censorship: historians of American foreign relations. For three years they have protested—mostly in vain—as State Department bureaucrats have found new rationales to prevent the disclosure of old, but not forgotten, diplomatic records.

The controversy, which so far has attracted little public attention, concerns the right of historians and interested citizens to the timely review of documents that tell the story of our government's recent diplomacy. At issue is the integrity of the State Department's invaluable documentary series, *Foreign Relations of the United States*, and the prolonged refusal of the department to release files from the early 1950s—files pertaining to the Korean War, the development of national security policy, covert operations abroad, and even the origins of American involvement in Vietnam. A series of restrictive policies beginning with the Carter administration and carried forward under Reagan threatens to keep the veil over these events. "The public's right to know thirty years after the fact what its government has done, or did not do in a specific area of the world is crucial to the functioning of a healthy democratic system," says one member of the State Department's historical office, which compiles the *Foreign Relations* series. "And that, I thought,

was the purpose of the *Foreign Relations* volumes when I got to the office. I have since realized that there are those in our office and outside who do not believe that is the mandate with which we've been charged and have no intention of carrying it out."

Some might argue that the public has a right to know what its government is up to long before thirty years go by. But the State Department guards its records so jealously that its declassification program lags behind even that of the notoriously reclusive British, who follow a strict thirty-year rule. The problem began, ironically, with the Carter executive order on declassification, which promised greater public access to materials of state. "The public is entitled to know as much as possible about the government's activities," President Carter declared on signing the order in June 1978. "The new order will increase openness in government by limiting classification and accelerating declassification. With a few exceptions, the documents . . . will be declassified after no more than twenty years."

Fine words, but as historians soon learned, empty ones. The effect of the order was to impose vast new bureaucratic obstacles to the release of documents. Previously, State had simply turned over masses of records to the National Archives for opening en bloc as soon as the annual *Foreign Relations* volumes were released. Now every sheet of paper had to be read and reviewed under restrictive guidelines prepared by the State Department's new Classification-Declassification Center (CDC), established to implement the order. No bureaucrat was going to risk letting anything sensitive through the strainer without higher review, so the process quickly ground to a slow crawl. "One of the

great ironies in all this is that the best set of directives for releasing classified information was written by [Nixon aides] Ehrlichman and Haldeman in 1972," commented Walter LaFeber, a prominent diplomatic historian at Cornell University. "The Carter administration was retrogressive, yet it promised open government."

The problem went beyond the executive order, of course. With the release of *Foreign Relations* volumes from



the late 1940s, American embassies abroad began complaining that some of the documentary revelations were causing political difficulties, particularly as evidence came to light of U.S. political manipulations. Italian citizens, for example, were shocked to learn that the United States had considered staging a military coup in the event that the Communist Party won a peaceful victory in the 1948 elections. The CDC, sensitive to these concerns, called in for further review volumes of the 1950 *Foreign Relations* series that had already been cleared and prepared for printing. As historians waited in vain for the volumes to appear, the censors went to work. "We heard that 20 to 25 percent of the 1952-54 materials were being removed," said LaFeber. "CDC said less than one percent, but then we asked about the Iranian coup of 1953. In some of the important sec-

JONATHAN MARSHALL is an associate editor of *Inquiry*. Scott Chan did some of the research for this piece.

jections, and manufacturing procedures." He warned that those who opposed such restrictions were "about to have that way of thinking washed away by the tidal wave" of public opinion, and went on to say that "the tides are moving, and moving fast, toward legislated solutions that in fact

are likely to be much more restrictive" than the voluntary controls he proposed. The "tidal wave" of public opinion may only, have been a figment of his imagination, but Inman's threat was chilling nonetheless. (Admiral Inman is no stranger to efforts to censor the work of scientists. As director

of the National Security Agency [NSA], he actively sought to control independent work in cryptography, going so far as to classify two privately developed inventions, one a voice scrambler, the other a cipher device. Both were declassified a few months later.)

The second prong of the assault was a letter by Deputy Secretary of Defense Frank C. Carlucci in the January 8 issue of *Science*, the weekly journal of the AAAS. "It is quite apparent," Carlucci argued, "that the Soviets exploit scientific exchanges as well as a variety of other means in a highly orchestrated, centrally directed effort aimed at gathering the technical information required to enhance their military posture." He cited three Soviet scientists who had obtained information he regarded as militarily sensitive while they were in the United States during the late 1970s: S. A. Gubin, who worked on concussion bombs; K. H. Rozhdavitskiy, who did research on aerodynamics; and T. K. Bachman, whose work was thought by some to have military applications for aircraft cockpit displays. Carlucci went on to note that in the Senior Scholar Exchange program "practically all the Soviet nominees propose to study in fields having military application . . . while the United States nominates scholars specializing in the arts, literature, and history."

tions, that 1 percent could be 30 to 40 percent of the material we desire. It just castrates the *Foreign Relations* series." Lloyd Gardner, professor of history at Rutgers and a leader in the fight for more openness, charges that the CDC is "lying with statistics" when it minimizes the impact of the deletions, since it is likely that the most revealing documents are those being censored. Inside sources at the State Department's historical office say that up to 17 percent of the documents included in the *Foreign Relations* series have been withheld, and that the largest deletions have come from materials on Western Europe, Korea and China, and the Middle East. The 1951 volumes on those areas have been delayed until next year.

Meanwhile, scholars will have a much longer wait for access through the National Archives to the general bulk of records from the 1950-54 period. Budget cuts at the Archives have reduced the declassification staff to one-third of its former size, and with document review made vastly more arduous by the demands of the CDC guidelines, Archives has so far refused to accept records from that period. Edwin Thompson, head of records declassification at Archives, now predicts only that the "larger part" of the 1950-54 records will become available by 1986 "if all comes through as we can best hope."

Even when the materials do become available, the most significant documents may well be missing. Intelligence-related records, in particular, are being withheld, which will color historical accounts of electoral and paramilitary intervention by the United States in Western Europe, the Soviet Union and the Balkan States, Guatemala, Iran, and the Far East. "After 1950 the intelligence aspect is more pervasive," says Neal Petersen, acting deputy historian at State, "and things get stickier and stickier." Adds Edward Becker, a private researcher with long experience at the

Archives, "You are going to get a very incomplete picture of what was going on, since the CIA was increasingly given charge of the implementation of U.S. foreign policy in that period."

The other major problem arises from an exemption in the Carter executive order for "foreign-originated information." Some State Department officials have interpreted the phrase to mean any information given in confidence by foreign officials. "Pushed to its limit [the exemption] might mean nothing would be released at all," admits Petersen. In practice, the exemption has been invoked to avoid embarrassing friends of the United States. "A sub-cabinet type in Italy in the 1950s might today be a defense minister," explains Petersen. "If he was rabidly pro-American that might hurt him now with the opposition." Pressed to come up with concrete examples of damage done by the release of materials through the *Foreign Relations* series, however, CDC officials could come up with only one case—an Icelandic politician who complained because of an adverse reference to him in the documents.

Meanwhile, the future looks bleak, with Reagan proposing in a new executive order to drastically broaden the scope of classification and eliminate mandatory review. "Everyone says things will tighten up under Reagan," says Petersen. "The atmosphere now is even worse," agrees Lloyd Gardner. "Under Carter, at least, a pretense was being made that there was to be openness in government. Supposedly his new guidelines were going to increase access. This didn't happen, of course. While Carter's executive order on paper promised openness," the bureaucracy thwarted its intent. "Now under Reagan the government at the top and the lower levels of the bureaucracy both are in accord on the need for more secrecy." □

THE SIGNIFICANCE OF these repressive fulminations was brought into focus the following week by the announcement that Stanford University would not accept the restrictions that the State Department, through the National Academy of Sciences, sought to place on the visit of Soviet roboticist Nikolai V. Umnov to the university's campus. Stanford Vice-Provost Gerald Lieberman, noting that the university no longer engages in classified research, stated: "There may be some technological leakage. But the solution will do more harm than good. The reason we are ahead in high technology is because of openness. If we can't exchange information, research will be harmed in a very counterproductive way."

The university's refusal was the result of prodding by Bernard Roth, professor of mechanical engineering, who was to be Umnov's host at Stanford. Roth was incensed by the severity of

the proposed restrictions on Umnov; he regarded them as significantly stricter than the controls previously imposed on other visiting Soviet scientists. Stanford has a number of foreign scholars currently in residence under much less onerous terms, and Roth found these new limits on what Umnov could see and do to have a certain "Alice in Wonderland" air about them.

The State Department retaliated against Stanford by blocking Umnov's visit altogether and then, only a week later, by denying permission for Soviet diplomat Yuri Kaprolov to visit the Stanford campus to participate in a forum on disarmament. The resulting public furor proved embarrassing to the government, however, and in early February the State Department finally relented on the Umnov visit. Umnov will now be allowed access to unclassified research funded by the Defense Department. Stanford is not alone in having to stand up to the government; the number of cases where controls have been rejected is large and growing. In 1981 the Massachusetts Institute of Technology refused to cooperate with attempts to limit the activities of a visiting Chinese physicist. And this January MIT rejected proposed restrictions on visiting Soviet chemist Mikhail Gololobov. The State Department ordered MIT to prevent Gololobov from seeing any work done in nutrition research. Since he was slated to visit the Department of Nutrition and Food Science, which does nothing but nutrition research, MIT officials were understandably dismayed. Similar protests of government meddling are under way at the University of Minnesota, the University of Wisconsin, and Ohio State University.

Should the administration seek to impose mandatory restrictions on the dissemination of scientific and technical information, it certainly has ample legal basis for so doing:

■ The Invention Secrecy Act of 1951 permits the Defense Department and the Patent Office to classify as secret any invention that they determine to be "detrimental to national security" should it be published. Approximately 300 patents are so classified each year, primarily military devices developed by government researchers.

■ The Atomic Energy Act of 1954 enables the Department of Energy to classify as "restricted data" any data or concepts pertaining to nuclear

weapons. As George Washington University law professor Matv Chelomnted at the AAAS symposium, the prosecution in the nuclear-secrets case against the *Progressive* "sought and obtained judicial support for the government's long-held view that the information control provisions may be applied to any information falling within the definition of Restricted Data regardless of where the information originated." Previously, however, the government had applied the information control provisions only to Restricted Data generated by government employees or under government support or sponsorship."

■ The Arms Export Control Act of 1976 allows the State Department to prevent the dissemination of "any unclassified information" pertaining to items included in the International Traffic in Arms Regulations (ITAR) list of munitions subject to export controls, as well as "any technology which advances the state of the art or estab-

lishing them. But the Reagan administration seems determined to exploit the broadness of the language to the fullest. Representative George E. Brown, Jr., a Democrat from Riverside, California, circulated a "Dear Colleague" letter to House members warning of the dangers of the administration's initiatives. But the degree of support Reagan enjoys in the Congress is cause for some pessimism. Representative Charles E. Bennett of Jacksonville, Florida, has introduced a resolution (H.R. 109) that would further extend the scope and restrictions contained in these last two laws, although congressional action is awaiting guidance from the executive branch.

The White House has drafted an executive order that would reverse decades of increased government openness.



lishes a new art in an area of significant military applicability in the United States."

■ The Export Administration Act of 1979 requires the Commerce Department to issue export permits for almost every item of commerce not on the ITAR list. The law prohibits the dissemination to foreigners, by any means, of "technical data," defined as "information of any kind that can be used, or adapted for use, in the design, production, manufacture, utilization, or reconstruction of articles or materials" unless an export license has been issued.

The broad language of these laws, which cover virtually every activity in American life, was enacted with congressional understanding that the executive would be circumspect in ad-

EVEN IF CONGRESS DOES not back Reagan, he can still impose mandatory information controls by executive order. The White House is studying a draft of just such an order, which would reverse three decades of increasing governmental openness, by changing the "balance of interests" test for deciding what information should be restricted. Heretofore, national security concerns had to be balanced against other interests. Under the drafted order, any information that has any national security implications would be restricted, regardless of how minor these implications, or how compelling the need for public disclosure. The order would do away with the current prohibition against classifying "basic sci-

entific research information not clearly related to national security." It would permit classification of non-governmental research prepared without access to classified information. It would eliminate any mandatory review of document classification. And, contrary to previous standards, it would impose on government bureaucrats the rule: When in doubt, classify.

Any attempt to further limit the free flow of scientific information will certainly face a number of obstacles. Current laws that would be the basis for mandatory legal controls are written in such vague and general language that they are probably vulnerable to successful challenge on constitutional grounds. Moreover, the government really lacks the organizational wherewithal to enforce such controls. However, scientists have put themselves out on a limb by accepting so much government financing. In fact, big government and big science are so intertwined that the imposition of mandatory controls would foster an adversary relationship that neither is anxious to see. Ira Michael Heyman, who worked with the NSA to develop review procedures for publication of research on cryptography, argued that "In the cryptography circumstance, I was willing to assume that the loss could be large and the amount that you are restricting people was very small. In the broader case, it seems to me it's just the opposite. Once you start to extend that principle . . . anything that's written in the sciences . . . is going to be swept into this system. It's much, much too broad."

The imposition of mandatory information controls also raises the specter of a "scientific samizdat," with scientists furtively passing on the results of their research to circumvent government controls. The widespread use of computer terminal networks would facilitate this process. But the impact on scientific progress would be devastating. According to William D. Carey, executive officer of the AAAS: "Our own military power will be diminished, not enhanced, if the well-heads of scientific communication are sealed and new knowledge confined in silos of secrecy and prior restraint." If the Soviet Union lags behind the United States in most fields of science, it is not for lack of brainpower, funds, or official support—but for lack of openness. "It is no accident that the United States has the widest technological

lead in those areas where government regulation has been the least," says Peter J. Denning, president of the Association for Computing Machinery.

These difficulties explain in part Admiral Inman's predilection for "voluntary" self-censorship. But to be effective, the volunteers must be persuaded of the need for controls. Carey of the AAAS says, "I have exceedingly great trouble accepting the proposition of making substantial concessions in the absence of a clear and present danger."

It is doubtful whether the few isolated examples of technological leakage to the Soviets add up to the menace the national security managers have conjured up. With the Pentagon Papers and the *Progressive's* publication of H-bomb schematics, the government's predictions of calamity have not been borne out by events. Advocates of censorship, learning from these mistakes, no longer cite specific damage from specific leaks of information but merely assert an undifferentiated menace to some vaguely delineated conception of national security. Needless to say, this formulation leaves many members of the scientific community unconvinced.

For one thing, America is not the only place the Soviets can gain access to advanced technologies. European scientific work is certainly on a par with that of the United States. And the Japanese lead the world in areas such as robotics and electronics.

A more basic question is whether secrecy can work at all. When the United States began developing the atomic bomb in the early 1940s, American scientists agreed to withhold their research on nuclear fission from publication. Soviet physicists were able to deduce from this suspicious silence that the United States was working on a bomb, and convinced their own country to do the same.

Professor Roth at Stanford thinks that the current control program is "administered by lawyers who don't understand technology" and "don't understand what they are doing." According to Mary Cheh, "some government administrators and policymakers believe that knowledge should be hoarded and traded like any other commodity." She notes that the true barrier to technology transfer is not acquisition of information, but "acquiring the cadre of skilled scientists

needed to reduce the information to application [and] building the sophisticated and expensive facilities needed for production."

American scientists have also expressed concern over the potential loss of technical information from Soviet scientists. Umov is a leading worker in the field of robotics, and in past years his contributions facilitated great advances in American robotics. American fusion research was greatly aided by information provided by Soviet scientists on their Tokamak reactor design. Planetary astronomers are worried that the Soviets might not share data and photographs from Venus acquired by their new "nereia" spacecraft.

INVOKING NATIONAL SECURITY as a pretext for censorship no longer satisfies most Americans. As Admiral Inman himself admitted, this suspicion "stems from a basic attitude that the government and its public servants cannot be trusted. I do not think it is harmful to recognize that the federal government—particularly its intelligence agencies—have in fact made mistakes in the past on occasion, and suspicion of the federal government in this regard is understandable." With some of the admiral's former employees going to work free-lance in Libya, carrying top-secret technology with them, perhaps he should clean his own house first.

National security consists of more than just military hardware. It derives from who we are as a people, and what we stand for as a nation. Much of America's greatness rests on our fundamental commitment to freedom, particularly freedom of speech. Admiral Inman's initiative strikes at the heart of that freedom. The basis of his proposal is "that which is not permitted, is forbidden." It is this totalitarian thought control that we find so abhorrent in Soviet society.

We must not miss sight of the larger issue. The threat of scientific censorship is part of a concerted attack on the First Amendment. The Intelligence Identities Protection Act and the assault on the Freedom of Information Act are part and parcel of an effort to destroy the cornerstone of American democracy. We must remember the words of physicist Niels Bohr: "The best weapon of a dictatorship is secrecy; the best weapon of a democracy is the weapon of openness." Q

FEDERAL RESTRICTIONS

ON THE FREE FLOW OF ACADEMIC INFORMATION AND IDEAS

JANUARY 1985

HARVARD UNIVERSITY

John Shattuck
Vice President
Government, Community
and Public Affairs

TABLE OF CONTENTS

Introduction	I
I. Prepublication Review and Contract Restraints	4
A. National Security Decision Directive 84	8
B. Government Sponsored Research	10
II. Increased Classification	14
III. Export Controls	19
A. Regulatory Scheme	19
B. Application to Universities	21
C. Atomic Energy Research	23
D. Current Policy Developments	26
IV. Restrictions on Foreign Scholars	29
Conclusion	32

Introduction

The freedom of scholars to express ideas and exchange them with colleagues is essential to the operation of universities in the United States and to maintaining the high quality of academic research. Academic freedom is rooted in the First Amendment to the Constitution, the same provision that protects the right of people to speak freely and the freedom of the media to report events as they see them.

Recent actions and proposals by some agencies of the federal government threaten to erode the American tradition of academic freedom. These proposals and actions fall into two broad categories -- those restricting dissemination of ideas and those restricting the access of foreign scholars to U.S. classrooms and laboratories.

In most instances, the justification given for these restrictions is the need to protect national security, an area in which technology plays an increasingly important role.

Responding to mounting government concern that technological information with potential military applications may be reaching the Soviet Union and other adversaries through industry and the scientific community, the National Academy of Sciences (NAS) issued a report in September, 1982 on Scientific Communication and National Security. The study was conducted by an NAS panel chaired by former Cornell University President Dale Corson. The authors expressed the hope that their recommendations would make it possible to "establish within the Government an appropriate

group to develop mechanisms and guidelines in the cooperative spirit that the report itself display[ed]."¹

Universities, which conduct most of the basic scientific research in the United States, were a primary focus of the NAS study. The report found "a substantial transfer" of U.S. technology to the Soviet Union, but concluded that "very little" of the problem resulted from open scientific communication.² Moreover, the report took note of the close connections between the American tradition of open communication, scientific and technological innovation, and national security. Despite this conclusion, NAS staff members reported this year that government policymakers are moving to implement new secrecy regulations before a government-wide consensus is reached.³ The staff also stated that where regulations already exist, policymakers are aggressively stretching their authority beyond its previous limits.

These secrecy regulations often go far afield of any reasonable definition of national security. Indeed, the requirements of prepublication review now reach several federal departments and agencies and areas of sponsored research which have no relationship to national security matters. Nor is the regulatory

¹ National Academy of Sciences, "Scientific Communication and National Security". Quoted from cover letter by NAS president Frank Press. This study is also known as the Corson Report.

² Id. at 1.

³ M. Wallerstein and L. McCray, "Update of the Corson Report", January 26, 1984, at 12.

scheme limited to research that is federally funded. Instead, it is being extended to broad categories of research and information -- such as cryptography and nuclear energy -- that are deemed to be so sensitive and important that the federal government must intervene whether or not it is paying for the research.

The movements afoot in Washington to restrict publication and dissemination of scientific research findings are matters of deep concern among members of the academic community. Similar concerns also arise over government restrictions on the activities of foreign scholars.

These concerns are addressed in the pages that follow.

I. Prepublication Review and Contract Restraints

Political philosophers have long maintained that the rights of free speech and of a free press are essential to the proper functioning of democracy. The importance of open communication in our society has been so compelling that courts have held that only an overwhelming danger "so imminent that it may befall before there is opportunity for full discussion" provides sufficient grounds for restraining free speech. If the danger or evil is not imminent, then the remedy is "more speech, not enforced silence."⁴

Until very recently, any proposed prior restraint on publication has come under a "heavy presumption against its constitutional validity."⁵ This presumption was so dominant that only narrowly focused government claims of national security during wartime could be balanced against it. For example, the Supreme Court held in Near v. Minnesota that publishing "the sailing dates of transports or the number and location of troops" would be the only kind of publishing activity the government could rightfully prevent in such circumstances.⁶

⁴ Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J. concurring).

⁵ United States of America v. The Progressive, Inc., 467 F. Supp. 990,992 (1979), quoting New York Times v. United States, 403 U.S. 713 (1971).

⁶ 283 U.S. 697,716 (1931).

As technology has come to play an increasingly important role in warfare and national defense, the traditional analysis of prior restraint issues has come into question. Many analysts have argued that U.S. security no longer depends on having "the largest military" or "the best-trained soldiers" but increasingly, rather, on a "technological lead over our military adversaries."⁷ This has led to a change in the focus of controls over exports "from goods to the technology used to produce those goods."⁸ One technique for achieving this new objective is pre-publication review.

In the past, only the CIA has used prepublication review, pursuant to contractual arrangements with its employees which implement its statutory mandate to "protec[t] intelligence sources and methods from unauthorized disclosure."⁹ CIA employees involved in covert intelligence operations have routinely had their speeches and writings reviewed for content that discloses classified information without authorization. The constitutionality of this specialized CIA practice was upheld in 1972 by a United States court of appeals in United States v. Marchetti.¹⁰

⁷ Testimony of Frank Press, President of the National Academy of Sciences before the U.S. House of Representatives subcommittee on Courts, Civil Liberties and Justice, November 3, 1983 at 4 and 5.

⁸ "Scientific Freedom and National Security", AAAS Bulletin, June 1984 at 7, summarizing the conclusions of the Bucy Report, "An Analysis of Export Control of U.S. Technology -- A DoD Perspective" (1976).

⁹ 50 U.S.C. Sec. 403 (d)(3).

¹⁰ 466 F. 2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972).

That decision did not, however, address whether prepublication review could be required for all material, including unclassified information.

The Supreme Court addressed this issue in 1980, in Snepp v. United States,¹¹ a case involving a former CIA agent who published a book criticizing practices of the United States during the Vietnam War.¹² All parties to the litigation agreed "that Snepp's book divulged no classified intelligence."¹³ Nevertheless, the Court held that Snepp had violated his agreement with the CIA by not giving "an opportunity to determine whether the material he proposed to publish would compromise classified information or sources." The Court awarded damages to the government in the form of a "constructive trust", into which Snepp was required to "disgorge the benefits of his faithlessness."¹⁴

The application of this decision has far-reaching consequences for academic research and publication. Two recent developments illustrate the point: 1) National Security Decision Directive 84, a Presidential order requiring all government employees (and contractors) with authorized access to certain

11 444 U.S. 507 (1980), (per curiam).

12 Snepp, Decent Interval.

13 444 U.S. at 510.

14 Id., at 515 (i.e. all book profits). Also, the Court found that Snepp had done "irreparable harm" to the Government because "the Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality..." at 509 and note 3. (Emphasis added.)

categories of classified information to sign lifetime prepublication review agreements as a condition of such access; and 2) the trend toward including prepublication review clauses in government-sponsored, university-based basic research contracts.

A. National Security Decision Directive 84

On March 11, 1983, the White House announced a security program designed to prevent unlawful disclosure of classified information by government employees. Since the date of its release, National Security Decision Directive 84 (NSDD 84) has generated a storm of controversy.¹⁵ Two of its provisions are particularly onerous. The first requires more than 120,000 government employees to sign nondisclosure agreements containing prepublication review clauses as a condition of access to certain categories of classified materials.¹⁶ The second permits government agencies to order polygraph examinations of agency personnel "when appropriate, in the course of investigations of unauthorized disclosures of classified information."¹⁷ It also requires each agency to promulgate regulations to "govern contacts between media representatives and agency personnel, so as to reduce the opportunity for negligent or deliberate disclosures..."¹⁸

15 "Reagan v. Madison", N.Y. Times, March 17, 1983; "The Who, What and Why of Reagan's Prepublication Review", N.Y. Times, March 27, 1983; "Men of Zeal", N.Y. Times, March 31. See also text of NSDD 84, Attachment A.

16 In a letter dated July 19, 1983, Deputy Assistant Attorney General Richard K. Willard noted that "the prepublication review provisions of the proposed [nondisclosure] agreement are similar to the agreement found by the Supreme Court to be enforceable in Snepp v. United States, supra. See also Alfred A. Knopf, Inc. v. Colby, 509 F. 2d. 1362 (4th cir.), cert. denied, 421 U.S. 992 (1975); United States v. Marchetti, supra; Agee v. CIA, 500 F. Supp. 506 (D.D.C. 1980)." (See letter attached at 3.)

17 NSDD 84 at 2.

18 Id., at 1.

In a recent Congressional hearing, Thomas Ehrlich, Provost of the University of Pennsylvania, described NSDD 84 as "virtually alone among important issues in recent times" in receiving a "completely uniform and completely negative...reaction of those in academia."¹⁹ Speaking for his own institution as well as for the Association of American Universities, the American Council on Education, and the National Association of State Universities and Land Grant Colleges, Ehrlich declared that he could not "overstate the dangers I see in the approach it adopts."²⁰ If fully implemented as issued, NSDD 84 would have "disastrous effects on the quality of our government in terms of those who enter and leave public service from academic life", Ehrlich stressed.²¹ It would, he said, cast a "deep freeze over any inducement for academics to serve in government by denying them the primary benefit of using government experience and information in scholarly publications and classroom lectures."²² Government would be deprived of academia's much needed expertise and insight. More important, the Directive would thwart criticism of government, since those "in the best position to provide that criticism" -- academics who have served in government and returned -- would be

19 Testimony of Thomas Ehrlich before the Committee on Governmental Affairs, United States Senate, February 23, 1984 at 1-2.

20 Id., at 2.

21 Id., at 4.

22 Id., at 5.

enjoined from discussing matters on which they had worked.²³ In view of academia's traditional role of providing a forum for criticism and debate, the restrictions in NSDD 84 would significantly reduce the scope of academic freedom.

Full implementation and enforcement of NSDD 84 is currently being held in abeyance as a result of a Senate resolution requesting further consideration by the Reagan Administration. The resolution expires at the end of 1984. While no government employees are currently required to take polygraph exams under NSDD 84, "120,000 employees have signed lifetime censorship agreements through Form 4193."²⁴

B. Government Sponsored Research

Most major universities receive funding for basic scientific and social research from the federal government. The funding is generally bestowed through contracts and grants between federal agencies and individual institutions. The terms of a contract or grant are subject to the statutory mandate and regulations of the funding agency.

In recent years, a growing number of federal agencies have inserted prepublication review clauses in university contracts, even those involving only unclassified material. For example,

²³ Id., at 6.

²⁴ See "Hear No Evil, Speak No Evil, Publish No Evil", N.Y. Times, August 16, 1984.

publication restrictions have been proposed for unclassified research to be performed under contract with the Department of the Air Force ("Measurement of Lifetime of the Vibrational Levels of the B State of N_2 "), the National Institutes of Health ("International Comparison of Health Science Policies"), the National Institute of Education ("Education and Technology Center"), the Department of Housing and Urban Development ("Study on Changing Economic Conditions of the Cities"), the Environmental Protection Agency ("Conference on EPA's Future Agenda"), the Health Resources and Sciences Administration ("Workshop for Staff of Geriatric Education Centers"), and the Food and Drug Administration ("Development of a Screening Test for Photocarcinogenesis on a Molecular Level").²⁵

Although prepublication review arose from national security concerns about the illicit transfer of technology to unfriendly governments, some of the most restrictive proposed contract clauses are contained in non-technological, social-research contracts. Apparently, federal agencies believe they can in this way insure that the research they fund is consistent with their view of their mission. The following is a clause from a proposed contract offered by the Department of Housing and Urban Development for university research on the use of housing vouchers:

Approval or disapproval (in part or in total) of the final report shall be accomplished by the CTR within thirty (30) days after receipt. Disapproved reports shall be resubmitted for review following correction of the cited

25

Examples of the publication restrictions proposed by these and other federal agencies are set forth as Attachments B-F.

deficiency unless otherwise directed by the contracting officer.²⁶

Consider another clause from a contract offered by the National Institute of Education:

The contractor shall not disclose any confidential information obtained in the performance of this contract. Any presentation of any statistical or analytical material or reports based on information obtained from studies covered by this contract will be subject to review by the Government's Project officer before publication or dissemination for accuracy of factual data and interpretation.²⁷ [Emphasis added.]

In addition, two other contract provisions referred to commonly as "Technical Direction" and "Changes" clauses, are used to alter the outcome of a given project. This is done either by direct participation in the project by a government official (technical direction) or by changing without notice the content and/or scope of the research contract without the researcher's agreement (changes clause).²⁸

Harvard's Office of Sponsored Research (OSR) reports success in negotiating changes in all three types of restrictive clauses. These negotiated changes enable the University to accept such contracts and perform them successfully. However, the Environmental Protection Agency in one instance has flatly refused to

-
- 26 Housing and Urban Development: Housing Voucher Demonstration Project.
- 27 National Institute of Education: Education and Technology Center Contract.
- 28 Pertinent clauses exemplifying such contracts are set forth in the attachments.

negotiate, offering a research contract only on a take-it-or-leave-it basis. But what is more important, OSR reports increasing resistance to negotiate deviations from standard agency provisions in all agencies. The University has accordingly refused some contracts.

In sum, the federal government is increasingly asserting an authority to require prepublication review of intellectual work by government employees, research universities and private citizens. As a result, the imposition of censorship has grown substantially beyond the boundaries of the traditional wartime national security exception to the ban on prior restraints that has long been a fundamental element of First Amendment doctrine.²⁹

²⁹ The government's direct and indirect interference with the presentation of research papers at scientific conferences is apparently accomplished through claims of contract and export control authority (Society of Photo-Optical Instrumentation Engineers [1982], 150 papers withdrawn; International Conference on Permafrost [1983], 6 papers withdrawn). For information on additional incidents of prepublication review and contract secrecy see Wallerstein, supra, at 10-11. The overall environment in which restrictive information policies are developing has also caused an increasing amount of self-censorship among scientists. The Washington Post recently reported that "[a] growing number of scientific and engineering societies are banning foreigners from their meetings for fear of violating federal rules against exporting strategically important technical information." Washington Post, December 15, 1984. See generally pp. 19-28, infra.

II. Increased Classification

President Reagan established the current system of security classification in 1982 by Executive Order 12356.³⁰ To grasp the import of this new system, one must first understand the security systems used by previous administrations.

Although the security classification systems used during the Truman, Eisenhower, Nixon, Ford and Carter administrations differed in their details, each contributed to a gradual trend toward government recognition of "the public's interest in the free circulation of knowledge by limiting classification authority, by defining precisely the purposes and limits of classification, and by providing procedures for declassification."³¹

The classification system designed by the Carter Administration³² was the culmination of this trend. It required government officials "to balance the public's interest in access to government information with the need to protect certain national security information from disclosure."³³ It stipulated that even if

30 E.O. 12356, 47 F.R. 14874 (April 2, 1982).

31 Rosenbaum, Tenzer, Unger, Van Alstyne and Knight, "Academic Freedom and the Classified Information System", Science Vol. 219, January 21, 1983 at 257.

32 E.O. 12065, 43 F.R. 28949 (June 28, 1978).

33 E.O. 12065, Preamble.

-15-

information met one of the seven classification categories³⁴, it was not to be classified unless "its unauthorized disclosure reasonably could be expected to cause at least identifiable damage to the national security."³⁵ [Emphasis added.] It provided for automatic declassification routinely after six years; only officials with "Top Secret" Security clearance classify a document for more than "twenty years".³⁶ Finally, it established a presumption such that "[i]f there is a reasonable doubt which designation is appropriate, or whether the information should be classified at all, the less restrictive designation should be used, or the information should not be classified."³⁷ [Emphasis added.]

Executive Order 12356 reverses this trend toward openness by significantly altering or eliminating each of the earlier systems' major features. The new order eliminates the balancing test: no longer must classifiers weigh the public's need to know against the need for classification. In addition, the threshold

³⁴ The categories were: "a) military plans, weapons or operations; b) foreign government information; c) intelligence activities, sources or methods; d) foreign relations or foreign activities of the U.S.; e) scientific, technological or economic matters relating to national security; f) programs for safeguarding nuclear materials or facilities; or g) other categories of information which require protection against unauthorized disclosure."

³⁵ E.O. 12065 Sec. 1-302.

³⁶ Id., Sec. 1; 1-4 Duration of Classification. Also, there is one exception to this rule: foreign-government information may be classified up to thirty years.

³⁷ Id., Sec. 1; 1-1 Classification Designation, 1-101.

standard for classification has been reduced. Heretofore, the classifier had to show "identifiable damage" to the national security.³⁸ The new executive order leaves much more room for discretion: it demands only that the classifier have a reasonable expectation of damage to the nation's security.³⁹ The new order also eliminates automatic declassification, requiring that information remain classified "as long as required by national security consideration."⁴⁰ Finally, the presumption in favor of openness is reversed. Now, "[i]f there is a reasonable doubt about the need to classify information, it shall be safeguarded as if it were classified...and [i]f there is a reasonable doubt about the appropriate level of classification it shall be safeguarded at the higher level of classification...".⁴¹

Secondary features of the security classification system have also undergone extensive revision in Executive Order 12356. In the areas of basic scientific research and reclassification, changes have taken place. Under both the new and the old executive orders, basic scientific research information unrelated to

38 E.O. 12065, Sec. 1-302.

39 E.O. 12356, Preamble: "Information may not be classified under this Order unless its disclosure reasonably could be expected to cause damage to the national security."

40 Id., Sec. 1.4(a), Duration of Classification.

41 Id., Sec. 1.1(c).

national security is exempt from classification.⁴² However, the initial drafts of the new order did not include the basic research exemption.⁴³ In addition, the previous order expressly limited the government's interest in non-governmental sponsored basic research⁴⁴ -- a matter that the new order leaves to administrative discretion.

Under President Carter's Order, "[c]lassification may not be restored to documents already declassified and released to the public...".⁴⁵ But under the new order, declassified information may be reclassified if "the information requires protection in the interests of national security; and [if] the information may be reasonably recovered."⁴⁶ Acting under this clause, the Reagan Administration unsuccessfully attempted in 1982 to recover documents previously released to a private researcher about electronic surveillance carried out by the CIA and NSA against anti-war activists in the 1970's. The documents had been provided to

42 Both Orders state: "Basic scientific research information not clearly related to the national security may not be classified." E.O. 12065, Sec. 1-602; E.O. 12356, Sec. 1.6(b).

43 "Academic Freedom and the Classified Information System", Supra, note 31, at 258.

44 E.O. 12065, Sec. 1-603: "A product of non-government research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified under this Order until and unless the government acquires a proprietary interest in the product."

45 E.O. 12065, Sec. 1-607.

46 E.O. 12356, Sec. 1.6(c).

author James Bamford, under a Freedom of Information request made in 1979.⁴⁷ Executive order 12356 provides that "information may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act or the Privacy Act...".⁴⁸ In contrast, the earlier order provided that "no document originated on or after the effective date of this Order may be classified after an agency has received a request for the document under the Freedom of Information Act..."⁴⁹

Given the bent toward secrecy exhibited by the many changes in the security classification system, scholars now fear that "[a]cademic research not born classified may, under this order, die classified."⁵⁰ The new order gives unprecedented authority to government officials to intrude upon academic research by imposing classification restrictions on areas of research after projects have been undertaken in those areas. The new order appears to allow classification to be imposed at any stage of a research project and to be maintained for as long as government officials deem prudent. Thus, the Order could inhibit academic researchers from making long-term intellectual investments in non-classified projects with features that make them likely

47 "The Rise of Government Controls on Information, Debate and Association", Free Speech, (1984) an ACLU Public Policy Report, at 11. Bamford refused to return the information. No other action was taken.

48 E.O. 12356, Sec. 1.6(d).

49 E.O. 12065, Sec. 1-606.

50 "Academic Freedom and the Classified Information System", Supra, note 31, at 258.

subjects for classification at a later date.⁵¹

III. Export Controls

A. Regulatory Scheme

In the area of export regulation, both military and civilian, statutory controls have been imposed over scientific communication related to basic research.⁵² These controls affect basic research through their definition of the terms "technological data" and "export". Information subject to export controls need not be classified, so long as it falls within the definition of "technological data" and is to be "exported".

The Export Administration Regulations (EAR), promulgated under the Export Administration Act of 1979, define "technological data" as "information of any kind that can be used, or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials. The data may take a tangible form, such as a model, prototype, blueprint, or an operating manual; or they may take an intangible form such as

⁵¹ Testimony of Dr. F. Karl Willenbrock, Chairman of the IEEE Technology Transfer Committee, before the House Judiciary Committee, Subcommittee on Courts, Civil Liberties and the Administration of Justice, Nov. 3, 1983, at 12.

⁵² Military Exports are regulated by The Arms Export Control Act, 22 U.S.C.A. Sec. 2751 et. seq.; Oct. 22, 1968 and The International Traffic in Arms Regulations, 22 CFR Sec. 121-130, Mar. 29, 1977. Civilian Exports are regulated by The Export Administration Act, 50 App., Sec. 2401-2420, Pub. Law 96-72, Sept. 29, 1979 and The Export Administration Regulations, 15 CFR Sec. 368-399.

technical service."⁵³ Under the Arms Export Control Act of 1963, the International Traffic in Arms Regulations (ITAR) contain an even more expansive definition of technological data, including anything that "advances the state of the art."⁵⁴

Both sets of regulations target areas of data through the use of lists. EAR creates the Commodity Control List.⁵⁵ ITAR creates the U.S. Munitions List.⁵⁶ The technological data related to any product that appears on either list are subject to export control. ITAR provides that information is "exported" whenever it is communicated overseas by "oral, visual or documentary means...", including "visits abroad by American citizens."⁵⁷ Under EAR, export means "(i) an actual shipment or transmission of technical data out of the United States; or (ii) any release of technical data in the United States with the knowledge or intent that the data will be shipped or transmitted from the United States...". Data may be released for export through "(i) visual inspection by foreign nationals...; [or] (ii) oral exchanges of information in the United States or abroad of personal knowledge or technical experience acquired in the United States."⁵⁸

⁵³ EAR 15 CFR Sec. 379.1(a).

⁵⁴ ITAR 22 CFR Sec. 125.01(b): "any technology which advances the state of the art or establishes a new art in an area of significant military applicability in the United States..."

⁵⁵ EAR Part 399, Commodity Control List and Related Matters.

⁵⁶ ITAR 22 CFR Sec. 121.01.

⁵⁷ ITAR 22 CFR Sec. 125.03.

⁵⁸ EAR 15 CFR Sec. 379.1(b)(1)(2).

B. Application to Universities

Historically, university researchers have been covered by exemptions (or general licenses) available under each set of regulations. ITAR specifically exempts information "in published form" or "sold at newsstands."⁵⁹ EAR gives such data a general license and also specifically allows "correspondence, attendance at or participation in meetings" and "instruction in academic laboratories" to be included under a general license.⁶⁰ However, these activities are allowable only so long as they do not relate "directly and significantly to design, production, or utilization in industrial processes."⁶¹ Until recently, routine academic activity has not been interpreted as being controllable under this clause.

In 1981, the Department of State sent a form letter to many universities inquiring into the study programs of certain Chinese foreign-exchange students.⁶² The authorities cited for this action were the Arms Export Control Act and the Export Administration Act.⁶³ In refusing to provide the information requested, Harvard University General Counsel Daniel Steiner character-

⁵⁹ ITAR 22 CFR Sec. 125.11(a)(1). A widely cited federal court of appeals decision, United States vs. Edler Industries, Inc., 579 F.2d516 (9th cir. 1978), has interpreted ITAR to have no applicability to unclassified research activity at universities.

⁶⁰ EAR 15 CFR Sec. 379.3.

⁶¹ EAR 15 CFR Sec. 379.3(2).

⁶² See Corson Report at 172-181; response by the University of Minnesota.

⁶³ Id., at 178.

ized the inquiry as "an interference into matters at the very heart of the academic enterprise." Other universities took similar actions.⁶⁴

The universities were not overreacting. Much of the requested information would have required close surveillance of student activities. The government wanted information on "professional trips" taken by students, "specific experiments" conducted on campus, and even information concerning "instruments or specialized equipment (e.g., lazer measuring devices, automated analytical equipment, computers, etc.) that may be used during the course of the study program."⁶⁵ The State Department made a similar inquiry about a Polish scholar at Harvard in 1982.⁶⁶

The debilitating effects on academic freedom of the new export regulations are dramatically illustrated by a course on Metal Matrix Composites, offered recently at UCLA, that was advertised in the course catalogue as restricted to "U.S. Citizens Only."⁶⁷ The restriction was required because the course material involved unclassified technical data appearing on the Munitions Control List (ITAR) and thus subject to export control.

⁶⁴ "University Refuses State Department Request", Harvard Crimson, Dec. 2, 1981. See also Corson Report at 180-181. In the widely publicized Umnov case, for example, Stanford University and the National Academy of Sciences objected to State Department restrictions on university research activities by foreign scholars.

⁶⁵ See copy of questionnaire.

⁶⁶ In this instance, no form letter was involved. The information appeared to have been gathered in person and/or by telephone.

⁶⁷ Wallerstein at 9.

C. Atomic Energy Research

The government also asserts broad authority to control scientific communication in the area of atomic energy research. The Atomic Energy Act regulates the "development, utilization and control of atomic energy for military and all other purposes."⁶⁸ In addition, a 1981 amendment to the Act authorizes the Secretary of Energy, with respect to atomic energy defense programs, to "prescribe such regulations...as may be necessary to prohibit the unauthorized dissemination of unclassified information."⁶⁹ [Emphasis added.] Although the Act also authorizes the creation of "a program for the dissemination of unclassified scientific and technical information...so as to encourage scientific and industrial progress"⁷⁰ [emphasis added], creation of such a program has been constrained by a Department of Energy regulation proposed in April 1983. The proposed regulation, "Identification and Protection of Unclassified Controlled Nuclear Information (UCNI)"⁷¹, would require that all UCNI be treated as "proprietary business information" within the regulated organization.⁷² Such organizations would have to take "reasonable and prudent" steps to protect UCNI from unauthorized disclosure. In

⁶⁸ The Atomic Energy Act of 1954, 42 U.S.C.A., Sec. 2012(a).

⁶⁹ Id., Sec. 2168(a)1. The A.E.C. was abolished and its powers transferred to D.O.E. in 1977.

⁷⁰ Id., Sec. 2013(b).

⁷¹ UCNI, 10 CFR Part 1017, F.R. 13990 et. seq., April 1, 1983.

⁷² Id., 10 CFR Sec. 1017.4(a).

addition, government contractors would have to assure that potential users have a "need to know", are U.S. citizens, or meet one of six other criteria.⁷³

In commenting on the proposed regulations, Stanford University, joined by Harvard, suggested a redrafting of the rules because of the major difficulty that they would cause for research universities. The proposed rules would require a university to make "known and unclassified information secret."⁷⁴ The Stanford comments pointed out that the proposed regulations would be so inclusive as to apply to materials used in "all those basic and advanced courses in fields of physics, electrical engineering, materials science and the like, that teach the basic information discovered and classified before the early 1950's and since declassified."⁷⁵ Most important, the commentators argued that restrictions requiring use of business standards in protecting proprietary material would interfere with basic research because of university policy that "such data be specifically identified in advance so that [it] can be certain its acceptance is consistent with...research guidelines."⁷⁶ Moreover, the regulations made no statement concerning new research-generated

73 Id., 10 CFR, Sec. 1017.4(b): 1) Federal employee; 2) contractor; 3) Member of Congress; 4) Governor of a state; 5) state or local law enforcement officer; 6) possessor of a D.O.E. Access Permit.

74 Comments of Stanford University, from the office of Gerald J. Lieberman, Vice Provost and Dean for Graduate Studies and Research, April 29, 1983, at 2.

75 Id., at 2.

76 Id., at 2.

UCNI. Stanford and Harvard asserted that this ambiguity would conflict with their fundamental policy that "all new information developed in the course of research be publishable."⁷⁷

On August 3, 1984 a new draft of the UCNI regulations was issued for public comment.⁷⁸ As a matter of principle, Harvard and other research universities continue to oppose federal restrictions on the dissemination of unclassified information. However, the new draft does contain improvements over its predecessor. Specifically, Harvard's comments on the new draft noted a "narrowed and better defined scope of application" of the proposed regulations. Also, the new draft contains an exemption for basic scientific information. Nevertheless, University commentators were careful to note the need for defining basic research so as to protect academic freedom. Specifically the Harvard comment suggested that basic research, exempt from all regulation, should be defined as: "information resulting from research directed toward increasing knowledge or understanding of the subject under study rather than any practical application of that knowledge."⁷⁹

⁷⁷ Id., at 2.

⁷⁸ UCNI, Proposed Rule; Notice of Public Hearing, 10 CFR Part 1017.49 F.R. 31236 (August 3, 1984).

⁷⁹ Comments of Harvard University, from the office of John Shattuck, Vice President for Government, Community and Public Affairs. (August 31, 1984) at 1.

D. Current Policy Developments

The debate over federal restrictions on the free flow of information and ideas has recently intensified in the area of export control regulations.

In October 1983, the House of Representatives adopted an amendment to a bill extending the Export Administration Act which provided that:

It is the policy of the United States to sustain vigorous scientific enterprise. To do so requires protecting the ability of scientists and other scholars to freely communicate their research findings by means of publication, teaching, conferences, and other forms of scholarly exchange.⁸⁰

However, the Senate version of the extension bill substituted the words "involves sustaining" for "requires protecting". More important, the Senate version inserted the word "non-sensitive" before the words "research findings".⁸¹ This key change substantially alters the meaning and intent of the entire paragraph. The Senate version would create the very restriction on scholarly exchange that the House version was intended to avoid. The Export Administration bill died at the end of the 98th Congress in October 1984 because no agreement could be reached in a House-Senate Conference Committee over a wide variety of issues in the bill. The new Congress is expected to take up the issue again in 1985.

⁸⁰ H.R. 3231.

⁸¹ Congressional Record, S 51722 (February 27, 1984).

Another recent development involves the Military Critical Technologies List (MCTL), which has been revised and expanded. This list is similar to the Commodity Control List and the U.S. Munitions list in that it designates sensitive applied technologies that the Defense Department desires to control. The list itself is classified, but a directive describing it states that the list now "covers all newly created technical documents generated by [DoD]-funded research, development, test and evaluation programs."⁸²

The MCTL is controversial for two reasons. First, it is statutorily incorporated into the Commodity Control List (CCL). Using the MCTL as a base, the Pentagon can propose changes in the CCL.⁸³ Second, the MCTL is reportedly over 700 pages long, and has been described by one DoD official as "really a list of modern technology"⁸⁴ and as a document that "could further complicate the use of these regulations as a means of trying to control scientific and technical communications."⁸⁵ The MCTL designates as "sensitive" technologies that the DoD desires to restrict.

In the area of contract controls, the "sensitive" designation arises in part from a "gray-area" identified by DoD offi-

⁸² Quoted in The Boston Globe, Nov. 4, 1984, at 9.

⁸³ See 50 App. U.S.C.A., Sec. 2404(a) 1,2,3,5.

⁸⁴ "Administration Grapples With Export Controls", Science, Vol. 220, June 1983, at 1023.

⁸⁵ Testimony of George H. Dummer, Director, Office of Sponsored Programs, Massachusetts Institute of Technology, before the House Subcommittee on Science and Technology.

cials "where controls on unclassified scientific information are warranted..."⁸⁶

The "gray area" approach, however, appears to have encountered opposition within the Defense Department itself. In testimony in May 1984 before the Subcommittee on Science, Research and Technology, Edith Martin, then Deputy Undersecretary of Defense for Research and Engineering, stated that DoD had decided "not to pursue the gray area concept because the option had proved to be more complicated than it had seemed."⁸⁷ She told the subcommittee that "[i]t is the policy of this administration that the mechanism for control of fundamental research in science and engineering universities and federal laboratories is classification..."⁸⁸ This statement was repeated on October 1, 1984 in a memorandum signed by then Under Secretary of Defense for Research and Engineering Richard DeLauer, stating that "no controls other than classification may be imposed on fundamental research and its results when performed under a federally supported contract."⁸⁹ The DeLauer memorandum was attached as a cover to a draft national policy on scientific and technical information. Whether the position articulated in the DeLauer memorandum will be formally adopted by the Reagan Administration must await the Administration's final action on the draft national policy itself.

⁸⁶ Wallerstein, at 18,19. Also non-sensitive/sensitive research would be distinguished by four criteria laid out in the Corson Report at 65.

⁸⁷ "DoD Springs Surprise on Secrecy Rules", Science, June 8, 1984, at 1081.

⁸⁸ Id., at 1081.

⁸⁹ Memorandum Concerning Publication of the Results of DoD Sponsored Fundamental Research, Reference DoD Directive 2040.2, October 1, 1984, at 1.

IV. Restrictions on Foreign Scholars

Under the Immigration and Nationality Act (known as "the McCarran Act"), foreign nationals can be denied entry into the United States because of their political and ideological beliefs.⁹⁰ The restrictive provisions apply to "aliens who...engage in activities which would be prejudicial to the public interest"; to "aliens who are members of the Communist Party" or "who advocate the economic, international and government doctrines of world communism"; and to "aliens who write or publish or cause to be written...printed matter...advocating or teaching... the economic, international and governmental doctrines of world communism."⁹¹

The leading Supreme Court decision interpreting the McCarran Act involved a Belgian journalist and Marxist theoretician, Ernest Mandel.⁹² Although not a member of the Communist Party, Mandel described himself as "a revolutionary Marxist".⁹³ Despite this description on all his visa applications, Mandel had been admitted to the United States temporarily in 1962 and again in 1968 before his first entry denial.⁹⁴ In 1969, he was invited to

⁹⁰ Immigration and Nationality Act, 8 U.S.C., Sec. 1101 et seq. (1952).

⁹¹ Id., Sec. 1182 (4), (5), (6), (9), (11), (12), (27), (28), (C), (D), (G).

⁹² Kleindienst v. Mandel, 408 U.S. 753 (1972).

⁹³ Id., at 756.

⁹⁴ Id., at 756. At those times, he was admitted under the waiver provision in Sec. (d)3(a).

speak at Stanford and he again applied for a six-day temporary visa.⁹⁵ The visa was denied on the grounds that his "1968 activities while in the United States went far beyond the stated purposes of his trip...represent[ing] a flagrant abuse of the opportunities afforded him to express his views in this country." Mandel and six U.S. citizens, all university professors, sued the United States.⁹⁶ The professors claimed that their First Amendment rights to hear and communicate with Mandel were being violated. A closely divided Court rejected the First Amendment claim.

The Mandel decision paved the way for a variety of entry denials or deportation proceedings against foreign born tenured professors at American universities. Three recent examples:

Dennis Brutus, a poet, writer and critic of apartheid, banned in South Africa for petitioning the South African Olympic Committee to allow black South Africans to compete on the national team. By attending a meeting of the South African Olympic Committee he violated the ban by being "with more than two people at a time." He was sentenced and served 18 months in prison. He came to the United States in 1970 to accept the teaching position at Northwestern University. His visa expired in 1980. He was required to obtain a permanent visa from outside the U.S. but because he had let his British passport expire this was not possible. He requested asylum. At his asylum hearing in 1983, Immigration Department lawyers used classified documents to make their case denying Brutus' attorneys access. Indirectly it

95 Id., at 757. He was also invited to Princeton, Amherst, Columbia, and Vassar after his scheduled visit became known. He then applied for a longer stay.

96 Id., at 759. The State Department conceded, however, that Mandel may not have been adequately informed of visa restrictions in 1968. See Id., at 773, note 4.

-31-

was learned that he was considered deportable under Sec. 212(a)(28) because of membership in the South African "Colored Peoples Congress". He was ordered deported but on appeal won asylum in late 1983.⁹⁷

Cosmo Pieterse, who came to Ohio State University in 1970 and was tenured in 1976. In 1979 he went to London to meet with his publisher and when attempting to return in 1981 was denied re-entry. This denial was based on classified information. It is believed that he has been denied entry for being a Communist even though his university colleagues deny this. He is still in London.⁹⁸

Angel Rama, a native of Uruguay, who made many trips to the U.S. before 1966. He was admitted on a regular visa until 1969 when he was apparently classified as a subversive and allowed to enter only on a waiver basis. In 1980 he earned tenure at the University of Maryland and applied for permanent residence status. The Immigration Department denied this request stating that the denial was based on "classified information...which [could] not be discussed...or made available..." Rama believed his denial was based on a series of articles he had written in the magazine Marcha, in which he reported on attempts by the CIA to infiltrate Latin American intelligence organizations. He was killed in a plane crash in Madrid before his case was resolved.⁹⁹

In addition to these university professors, a wide variety of foreign speakers invited to address university audiences in the United States have been denied entry from time to time in recent years under the "prejudicial to the public interest" pro-

⁹⁷ See "The Denial of Visas Under Sections 212(a)(27) and (28), The Ideological Exclusionary Clauses of the Immigration and Nationality Act", prepared for Representative Barney Frank (D-MA) by Emily McIntire, 1983 (unpublished manuscript) at 3-5.

⁹⁸ Id., at 7-9.

⁹⁹ Id., at 10-12.

vision of the McCarran Act. Among these are Nobel prize-winning authors Gabriel Garcia Marquez and Czeslaw Milosz, as well as author Carlos Fuentes, playwright Dario Fo, actress Franca Rame, NATO Deputy Supreme Commander Nino Pasti and Hortensia Allende, widow of former Chilean President Salvador Allende.¹⁰⁰

Conclusion

The free flow of ideas among scholars and their colleagues is essential to the fabric of academic life. The foregoing discussion shows the extent to which federal authority is now being asserted to restrict and disrupt that flow.

¹⁰⁰ Id., at 17.

APPENDIX 3

APPENDIX I—ARTICLES

- A. Soma & Wehmhoefer, "A Legal and Technical Assessment of the Effect of Computers on Privacy," 60:3 Den L.J. 449 (1983).
- B. "The High-Tech Threat to Your Privacy," Changing Times, April 1983, at 61.
- C. Dubro, "Your Medical Records. How Private Are They?" California Lawyer, April 1983, at 33.
- D. Neustadt & Swanson, "Privacy and Videotex Systems," Byte, July 1983 at 98.
- E. Smith, "Probing the Capitol's Drug Store," 9 Privacy Journal, September 1983. Attachment: Advertisement for Computerized Prescription System at Giant Pharmacies
- F. Boorman & Levitt, "Big Brother and Block Modeling," New York Times, Nov. 20, 1983.
- G. Boorman & Levitt, "Block Models and Self-Defense," New York Times, Nov. 27, 1983.
- H. Rule, McAdam, Stearns, & Uglow, "Documentary Identification and Mass Surveillance in the United States," Social Problems, December 1983, at 222.
- I. Clymer, "Privacy Threats Worry Americans," New York Times, Dec. 8, 1983.
- J. Burnham, "IRS Starts Hunt for Tax Evaders, Using Mail-Order Concerns' Lists," New York Times, Dec. 25, 1983.
- K. Brownstein, "Computer Communications Vulnerable as Privacy Law Lag Behind Technology," 16 National Journal 52 (1984).
- L. Burnham, "IRS Seeks Links to County Computers in Texas to Find Debtors," New York Times, March 13, 1984.
- M. Burnham, "U.S. Agencies to Get Direct Link to Credit Records," New York Times, April 8, 1984.
- N. Grier, "Who's Snooping and How? U.S. and U.S.S.R. 'Peer Into Mist'," (pts. 2-6), Christian Science Monitor (Apr. 17, 18, 19, 20, 23, 1984).
- O. Earley, "Government to Share Deadbeat List With Private Credit-Rating Bureaus," Washington Post, Apr. 25, 1984.
- P. Shattuck, "Computer Matching is a Serious Threat to Individual Rights," 27 Communications of the ACM 538 (June 1984).
- Q. Burnham, "IRS Rejected in Hunt for Estimated Income Lists," New York Times, Oct. 31, 1984.
- R. University of Maryland, Center for Philosophy & Public Policy, "Privacy in the Computer Age," QQ, Fall 1984.

APPENDIX II—MISCELLANEOUS MATERIAL

- A. The Direct Mail/Marketing Association's "Suggested Guidelines for Personal Information Protection" (1982).
- B. National Defense University, Department of Defense Computer Institute, "Selected Computer Articles 1983-84".
- C. Yudovich, "Administrative Surveillance—A Means of Police Repression," Dec. 6, 1983 (translation prepared by Radio Liberty Research (RL-454/83)).
- D. Marx & Reichman, "Routinizing the Discovery of Secrets," 27 American Behavioral Scientist, March/April 1984, at 423.
- E. Letter to Hon. Robert W. Kastenauer from Robert A. McConnell, Assistant Attorney General, U.S. Department of Justice, dated Mar. 30, 1984.

A LEGAL AND TECHNICAL ASSESSMENT OF THE EFFECT OF COMPUTERS ON PRIVACY

JOHN T. SOMA* AND RICHARD A. WEHMHOFER**

INTRODUCTION

Alexander Solzhenitsyn observed that "as every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man."¹ Computer technology collects, combines, and analyzes these threads in an efficient and timely manner.² An increasing amount of information is being collected by government and private industry. This information includes data collected from census and tax files, medical and credit reports, arrest and criminal records, and magazine subscription files. When accumulated in centralized data files, this information has the potential of being used as an instrument of control or, at the very least, may be used to trace and regulate an individual's movements and activities.³ Many commentators are concerned that the computer's insatiable appetite for information, image of infallibility, and eternal memory may cause it to become the heart of a surveillance system that will make society a transparent world in which our homes, finances, and associations will be bared to a wide range of observers.⁴

The use of collected data, however, is indispensable in our modern society. Personal information in both individual and aggregated contexts is in-

* J.D., Ph.D., Associate Professor of Law, University of Denver, College of Law. B.A., Augustana College; J.D., M.A., Ph.D., University of Illinois, Urbana. Dr. Soma is currently completing a book on Computer Technology and the Law for Shepard's/McGraw-Hill.

** J.D., Ph.D., associated with Akolt, Dick & Akolt, Denver, Colorado. B.A., M.A., Ph.D., University of Colorado, Boulder; M.P.A., Graduate School of Public Affairs, University of Colorado, Denver; J.D., University of Denver, College of Law. Dr. Wehmhofer is currently writing a book on Practical Statistics for Lawyers.

1. Linowes, *Must Personal Privacy Die in the Computer Age?*, 65 A.B.A. J. 1180 (1979). A fundamental issue of privacy is the amount of freedom each individual possesses. Freedom is of course directly related to the number of people in a defined space. Herbert wrote that beyond a critical point,

within a finite space, freedom diminishes as numbers increase. This is as true of humans in the finite space of a planetary ecosystem as it is of gas molecules in a sealed flask. The human question is not how many can possibly survive within the system, but what kind of existence is possible for those who do survive.

F. HERBERT, DUNE 493 (1965).

2. See generally A. MILLER, *THE ASSAULT ON PRIVACY* (1971); A. WESTIN, *PRIVACY AND FREEDOM* 158-68 (1967); Bazelon, *Probing Privacy*, 12 GONZ. L. REV. 587 (1977).

3. See A. MILLER, *supra* note 2, at 38-46. This fear resulted in considerable opposition to both the government's proposed National Data Center in 1967 and President Reagan's proposal in 1981 to create a centralized data file in the Department of Health and Human Services in order to track welfare recipients.

4. See, e.g., V. FERKISS, *TECHNOLOGICAL MAN* 227 (1969); Miller, *The National Data Center and Personal Privacy*, *THE ATLANTIC*, Nov. 1967, at 53; *Osborn v. United States*, 385 U.S. 323, 353 (1966) (Douglas, J., dissenting); *Lopez v. United States*, 373 U.S. 427, 450 (1963) (Brennan, J., dissenting).

creasingly needed to understand and formulate policies to solve social, economic, and political problems. Prior to the development of the computer, vast data collection and interpretation were not possible.⁵ Some contemporary prophets have predicted that the advent of these new information transfer technologies will prove to be as significant as the invention of movable type.⁶

An inherent problem in the development of computers is its effect on individual privacy. This article will examine that effect from historical, contemporary, and futuristic perspectives. It will also evaluate contemporary constitutional, judicial, and statutory responses to the protection of individual privacy in the United States and internationally.

The simplest definition of privacy was stated by Justice Brandeis in his dissent in *Olmstead v. United States*.⁷ He said that privacy is "the right to be left alone."⁸ Other more comprehensive definitions of privacy include Professor Westin's statement that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."⁹ Professor Emerson noted that "[t]he right of privacy, in short, establishes an area excluded from the collective life, not governed by the rules of collective living."¹⁰ In this article, privacy will be defined as the unitary concept of separation of self from society.¹¹

I. COMPUTER TECHNOLOGY DEVELOPMENT AS RELATED TO PRIVACY

After World War II, the United States witnessed a tremendous expansion of commercial and governmental activities, which resulted in a substantial increase in the volume of transactions requiring the maintenance of records on individuals. The number of bank checks written doubled and the

5. Ruggles, *Symposium: Computers, Data Banks, and Individual Privacy: On the Needs and Values of Data Banks*, 53 MINN. L. REV. 211, 233 (1968).

6. A. CLARKE, *PROFILES OF THE FUTURE* 265-79 (1962); H. KAHN & A. WIENER, *THE YEAR 2000*, at 88-98 (1967); M. McLuhan, *THE GUTENBERG GALAXY* 11-279 (1962); A. WESTIN, *supra* note 2, at 163-68.

7. An example of the scientific community's views of the impact of the computer on our society is the following excerpt from a speech by Dr. Glenn T. Seaborg, Chairman of the United States Atomic Energy Commission, reprinted in *Computer Privacy: Hearings Before the Subcomm. on Administrative Practice and Procedure, Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. 248 (1967):

Springing from our Scientific Revolution of recent decades is what is being called our "Cybernetic Revolution." This revolution which, comparatively speaking, is only in its infancy today amplifies (and will to a large extent replace) man's nervous system. Actually, this is an understatement because computers amplify the collective intelligence of men--the intelligence of society--and while the effect of the sum of man's physical energies may be calculated, a totally different and compounded effect results from combining facts and ideas Add this effect to the productive capacity of the machine driven by an almost limitless energy source like the nucleus of the atom and the resulting system can perform feats almost staggering to the imagination. That is why I refer to cybernation as a quantum jump in our growth

7. 277 U.S. 438 (1928).

8^o *Id.* at 479 (Brandeis, J., dissenting)

9. A. WESTIN, *supra* note 2, at 7.

number of income tax returns quadrupled.¹² Automated data processing blossomed into a separate industry, serving the demands of business and industry for fast, accurate, and efficient data handling.¹³

During the late 1960's, business and social planners began to use the concept of systems analysis, which involves the mathematical simulation of a complex activity or task. Systems analysis was applied to problems concerning health care delivery, income transfer payments, air pollution, urban transportation, and higher education. The introduction of the disciplined methods of computer-assisted management gave business and social planners new tools for evaluating the performance of programs and institutions dealing with social problems. This auditing process included tracking transactions between organizations and their clients, measuring performance against goals, providing information for planning, and assessing workload and productivity.

Many of these functions necessarily involved the collection and storage of data on individuals. For example, administrative data were needed for management of individual transactions and statistical data were needed for planning and assessing program performance. Intelligence data were needed for judging individual character and qualifications for employment, credit, welfare assistance, and other aid. Health data were needed to provide adequate health care and medical assistance. The demand generated by all these uses of personal data, and the corresponding record-keeping systems to store and process this information, challenged conventional legal and social controls to protect individual privacy.

Computer technology can be expected to continue to improve the capacity, speed, and complexity of storing and analyzing data concerning individuals. The federal government continues to sponsor the development of advanced computer systems for the military and space programs. Strong, world-wide economic pressures exist for automating various operations in the public and private sectors. Public opinion is becoming increasingly receptive to the provision of better data and faster information processing. There has been a tremendous infusion of venture capital into computer development to the extent that this has been described as the "last frontier of entrepreneurial capitalism."¹⁴

Given this pattern of rapid innovation and technological development, policymakers have legitimate concerns that computer technology can severely impinge on individual privacy. As early as 1972, Professor Westin found that computer technology existed that could maintain an on-line file containing the equivalent of twenty single-spaced pages of typed informa-

12. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 7-10 (1973).

13. See generally B. GILCHRIST & R. WEBER, THE STATE OF THE COMPUTER INDUSTRY IN THE UNITED STATES 54 (1973); M. HOLMIEN, COMPUTERS AND THEIR SOCIETAL IMPACT 43-44 (1977); E. TOMESKI & H. LAZARUS, PEOPLE-ORIENTED COMPUTER SYSTEMS: THE COMPUTER IN CRISIS 130-32 (1975).

14. Michael Shields, a catalogue marketer for Apple Computers said that "living [in the Silicon Valley of northern California] is like riding in the nose cone of the space shuttle. We are

tion about the personal history and selected activities of every man, woman, and child in the United States.¹⁵ It would have been possible to retrieve this information on any given individual within thirty seconds.¹⁶

Although Americans enjoy the convenience and speed of information processing, a recent Harris poll found that nearly two-thirds of those interviewed were concerned about threats to their privacy; one-third said that the United States is or would soon be similar to the fictional "Oceania" in George Orwell's novel *1984*¹⁷—a nation that kept every activity of its citizens under constant surveillance.¹⁸

A. Major Areas of Computer Technology That Will Affect Privacy

1. Input

Direct-entry input devices and optical scanning methods represent techniques by which data, either numeric or alphabetic, can be entered directly into machine-readable form. Some forecasters believe voice input devices will become widespread by the late 1980's.¹⁹

2. Storage

Larger memory storage capacities are being developed to place great volumes of personal data into direct-access storage for on-line access. These new techniques include laser beam technology allowing data to be stored at the molecular level.²⁰

3. Configuration Arrangements

More flexible options are available for arranging the configuration of computer systems. Included in this array are minicomputers and personal microcomputers which can be used for self-contained record-keeping and data processing applications. There are also improved capacities for linking terminals into on-line systems, thereby giving greater flexibility to organizations and government. Some organizations have become more decentralized in their record-keeping activities while others have elected to use large, multi-terminal centralized systems.²¹

4. Data-base Management Software

Considerable improvement is expected in data-base management

15. A. WESTIN & M. BAKER, *DATABANKS IN A FREE SOCIETY* 337-406 (1972).

16. *Id.* at 321-30. While there may not exist a single giant databank to hold all this information, it is possible to link separate computer systems within a separate organization or between organizations. Given the linkage technology already available, and if problems of common personal identifiers, compatible record formats, and appropriate software instructions for the desired use could be worked out, there would never be a need for one central processing unit to operate this data system.

17. G. ORWELL, *1984* (1949).

18. *Report on Privacy: Who is Watching You?* U.S. NEWS & WORLD REP., July 12, 1982, at 34-37.

19. *To Each His Own Computer*, NEWSWEEK, Feb. 22, 1982, at 50.

20. *Science Fiction: Reading The Future* 162 NATIONAL GEOGRAPHIC 921 (1982).

software. The movement toward management information systems allowing separate data files to be unified and processed will continue. Some experts believe the continued upgrading of those systems will depend largely on an improved understanding of business, social, and political processes, and major administrative reforms within these organizations.²²

5. Availability of Computers

The development of low-cost personal computers and relatively inexpensive terminal links into commercial time-sharing services has greatly increased the availability of computers to individuals and small organizations. In 1980, over \$1.8 billion was spent worldwide on personal computers.²³ Almost 2.8 million computers were sold in 1981 at an average cost of approximately \$2,000 each.²⁴ Predictions for 1985 are that over 50 million personal computers will be sold worldwide.²⁵ As computers become more readily available to individuals, more personal data will be accessible in machine readable form.

6. Communication Systems

Less expensive and more specialized communications systems for data transmission have been developed.²⁶ Microwave systems, satellites, cable television, and laser communications have been, or will be, developed for regular use.²⁷

7. Output Devices

More flexible and less expensive computer output technology has been developed. Computers will more frequently be used as "support" for microfilm and microfiche systems. Consequently, the sorting and preparing of hard-copy media through computer-output-to-microfilm devices will continue to grow.²⁸ Hardware costs will continue to decline, however, the cost of increasingly complex software systems will rise.²⁹

These technological advances make the computer essential for coping with the "information explosion."³⁰ It has been estimated that by 1987, six to seven times the present volume of new information will be produced, however, the ability of computers to automate the information may approach

22. Interview with Timothy Skinner, Staff Attorney, Lowery Air Force Base, Denver, Colo., (Dec. 22, 1982) (federal legal information through electronics).

23. *TIME*, Jan. 3, 1983, at 14.

24. *Striking it Rich*, *supra* note 14, at 41.

25. *To Each His Own Computer*, *NEWSWEEK*, Feb. 22, 1982, at 50.

26. The break up of AT&T on January 8, 1982 will lead to the continued development of telecommunications systems capable of providing efficient and effective methods for data transmission. *See, e.g.*, *ATLANTIC*, May 1979, at 68.

27. G. BROCK, *THE TELECOMMUNICATIONS INDUSTRY* 254-86 (1981).

28. NATIONAL ACADEMY OF SCIENCES, *LIBRARIES AND INFORMATION TECHNOLOGY: A NATIONAL SYSTEM CHALLENGE* 73 (1972).

29. *The Tail that Wags the Dog*, *NEWSWEEK*, Feb. 22, 1982, at 55.

30. *See, e.g.*, *N.Y. Times*, Sept. 9, 1979, § 3, at 1.

one hundred times the current capacity.³¹

B. *Major Issues Resulting from Computer Development*

Computer development and the projected use of computer technology carry many implications for society. Four issues which have been raised concerning this impact are automation, power, individuality, and privacy.³²

1. Automation

Just as the Industrial Revolution enhanced man's physical strength with machines, computational technology has begun to supplement some aspects of human thought processes. Computers are doing work that some people consider to be burdensome, tedious, and boring.³³ As a result, productivity and production costs have been optimized.³⁴ Some observers believe that computers create more jobs than they displace, while others theorize that computers will eventually destroy many more jobs than are created.³⁵

2. Power

It is said that "information is power." Computers create the potential for a few individuals to accumulate large amounts of data that can be readily accessed. Sophisticated computers create a power gap between those persons technically trained to interpret and use this information and those who do not have such skills. Computers can also dictate our actions. Systems failures, for example, can result in confusion and catastrophe. Recent system failures such as the blackouts in New York City, the accident at Three Mile Island, and air traffic control problems in Southern California have created chaotic situations.³⁶

3. Individuality

In the United States, the right to pursue happiness has historically been highly valued. Computers have significantly altered this emphasis on individuality. At times, our very essence is reduced to numbers on a terminal screen. Computers store aggregations of data such as fiscal and credit transactions, medical records, consumer habits, and communications. With access to so much accumulated data, however, social planners might easily begin to envision a society with goals that can be dealt with in mass, rather

31. See SCIENCE NEWS, Oct. 4, 1975, at 220; Etzioni, *Effects of Small Computers on Scientists*, SCIENCE, July 11, 1975, at 93.

32. W. MATHEWS, *MASTER OR MESSIAH? THE COMPUTER'S IMPACT ON SOCIETY* 32-36 (1980).

33. Robots are used to weld and attach machine parts for automobiles, steel work, electronic circuits, and other assembly line products. Japan has developed robots to build other robots. See *Japan's High-Tech Challenge*, NEWSWEEK, Aug. 9, 1982, at 48.

34. See TIME, Dec. 8, 1980, at 72-83.

35. *Machines Smarter than Men? An Interview with Robert Weiner*, U.S. NEWS & WORLD REP., Feb. 24, 1964, at B4.

than in terms of the individual.³⁷

4. Privacy

Some observers have argued against the trend to link data banks and access information on individuals because such trends could serve as the beginning of "individual data images."³⁸ In particular, Professor Westin has argued that existing computational technology capable of integrating several data banks into networks would allow personal data provided by an individual for one purpose to be used at a later time for unrelated purposes.³⁹ The likelihood that an individual would realize, much less approve of, such uses is remote.

There appears to be little legal or social movement at this point to place additional protections on privacy. Professor Westin has observed that privacy is a quality-of-life issue that is usually considered less important than economic and foreign policy concerns.⁴⁰

II. THE THREAT TO PRIVACY

The threats posed to the individual from computer technology have been described by one commentator as: illicit access to personal information; unexpected consequences of making information freely available by mechanical means; use of information for purposes other than those for which it was collected; actions based on inaccurate or outdated information; placement of the individual at a disadvantage as compared to organizations with ready access to large amounts of computerized information; and the undue credence given to information merely because it is stored in a computer.⁴¹ Other threats include the "secrecy" of personal information; unauthorized or illicit collection methods and omissions; the visibility of the data collection and analysis process; and the regulation of computers.⁴²

Another commentator has observed that the major effect of the computer on privacy is the removal of the individual from the decision of whether personal information may be released.⁴³ This loss of control can take two forms: loss of access control and loss of accuracy control.⁴⁴ When an individual is the sole source of information, he has at least some control over what information is disseminated to others. The advent of the computer databank added a new source of personal information over which the individual has no access control. Related to this development is the individual's diminished control over the accuracy and reliability of the personal information that is released through computer databanks.

37. A. VAN TASSEL, *THE COMPLETE COMPUTER* 153 (1976).

38. Koehn, *Privacy, Our Problem for Tomorrow*, *J. OF SYS. MGMT.*, 8-10 (July 1973).

39. *See* A. WESTIN, *supra* note 2, at 111-67, 317-54.

40. *Id.* at 14-20.

41. Barron, *People, Not Computers*, in *PRIVACY* 320 (J. Young ed. 1978).

42. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *POLICY ISSUES IN DATA PROTECTION AND PRIVACY* 148 (1976).

43. Beane, *The Right to Privacy and American Law*, 31 *LAW & CONTEMP. PROBS.* 233 (1966).

A. *Key Forces Threatening Privacy*

As computer technology improves, the ways in which privacy may be invaded increase. There are four forces in America that compel the need for legal protections of privacy.⁴⁵

1. Eavesdropping

There are increasingly more sophisticated devices available for eavesdropping. Professor Westin documented both governmental and private sector actions geared to secretly penetrate private places and intercept private conversations.⁴⁶ The assumption that persons can carry on a conversation in a home or room in private, is apparently no longer justified.

2. Sophisticated Databases

When records were kept on paper and requests for information had to be manually processed in writing, central files combining credit information, employment histories, and arrest records were unknown. The past as well as the present could be hidden or forgotten unless someone had the time and resources necessary to conduct an exhaustive search. Today, government and business maintain extensive records in computer databanks. Management information systems allow computers to be linked together to provide a comprehensive picture of a person's finances, employment, education, and reputation. Such systems are not immune from being tapped and having information stolen, nor does anything exist to prevent those with legal access from checking the records of selected individuals.⁴⁷

3. Growing Need for Information

As the ability to process information becomes greater, the public's perception of the need for additional data expands. Professor Miller attributes the explosion of information-keeping not only to advances in computer technology, but also to the federal government's entry into the areas of taxation and social welfare.⁴⁸ Many governmental agencies are beginning to ask complex, probing, and sensitive questions. Some of these questions have required the disclosure of a person's associations, medical history, and attitudes toward various institutions and people.⁴⁹ Similar trends are apparent in social science and private market analysis research where lie detector tests and personality examinations have been used to gather data relating to such private domains as a person's sexual preferences, religious beliefs, and other personal habits.⁵⁰

45. See Bazelon, *supra* note 2, at 597-600 (1977).

46. See A. WESTIN, *supra* note 2, at 158-68.

47. See, e.g., U.S. NEWS & WORLD REP., *supra* note 18, at 34-37.

48. See generally A. WESTIN, *supra* note 2, at 158-68.

49. See A. MILLER, *supra* note 2, at 21.

4. Increased Regulation

As the population grows and resources diminish, individual economic freedom will probably give way to increased governmental intervention. While this larger role for government may be condemned in principle, demands for economic security, education, adequate health care, and improved criminal justice systems require increased governmental involvement. The danger is that, while providing some benefits, the government will exert unnecessary controls that diminish individual autonomy and privacy.⁵¹

Bazon argues that the law must increasingly intervene to guard against the erosion of privacy through administrative regulations, statutes, and the common law.⁵² Whenever law affecting privacy is made by the courts, legislature, or executive branch, policymakers should engage in similar sorts of analysis to mediate among the inevitable competing interests.⁵³ This, according to Bazon, is probably the only way to protect privacy in the future.⁵⁴

B. *Types of Personal Information*

The use of computers to store personal information is exemplified by three *hypothetical* composite cases in which a loan, a life insurance policy, and a credit card are rejected. Although these cases are hypothetical, they typify the extent to which information can be used and abused once the data is stored in a computer.

John Smith, a forty-year-old engineer and honorably-discharged veteran, was denied a Veterans Administration (VA) guarantee on a home mortgage. He asked to review his file at the savings and loan association where he applied for the loan. The accepted banking practice in the United States is to permit the applicant to review only the file, not the credit report or the home appraisal.⁵⁵ Smith's review of the file revealed that he was convicted of a felony in 1965. The bank official told him that the credit report contained other adverse information and gave him the name of the credit reporting agency that supplied this information.

Smith and his attorney called the credit reporting agency. Under the Fair Credit Reporting Act,⁵⁶ Smith has the right to review his entire file, except for the medical information.⁵⁷ Credit reporting agencies generally base credit reports on contacts with their customers who have requested reports on individuals over the past years. They also contact references sup-

51. Some social commentators criticize Westin's notions of privacy and individualism as antagonistic to the general welfare. See J. Benn, *Privacy, Freedom, and Respect for Persons*, PRIVACY NOMOS XIII 18-23 (1971).

52. Bazon, *supra* note 2, at 600.

53. A. WESTIN, *supra* note 2, at 370-77.

54. *Id.*

55. Banks generally consider credit reports and appraisals to be their own information. When a potential customer completes a credit application, he consents to the bank's consultation of practically any person or institution about his credit, character, and general reputation. See

56. 15 C.F.R. § 1601 (1970).

plied by the credit applicant. These references are usually friends, merchants, and banks who have a record of the applicant's purchasing habits. Information from these sources, as well as from such court records as divorce decrees, garnishments, or bankruptcy documents, are then supplied to a requesting party such as the savings and loan association.

To Smith's surprise, his file contained a notation that he had been identified as a person known to have attacked or ridiculed a major doctrine of the Christian faith and the American way of life. As required by the Fair Credit Reporting Act, the credit reporting agency reinvestigated this notation after Smith protested.⁵⁸ It concluded that the notation, based solely on the fact that Smith's father had been investigated in the 1950's by the House Subcommittee on Un-American Activities, was not applicable to him. The agency, therefore, deleted the notation from his file and notified the savings and loan association.

The alleged felony conviction was, in fact, a conviction for civil disobedience when Smith was involved in a sit-in as a civil rights worker in the South. The bank obtained this information from Smith's veteran's files. The veteran's files also contained the name and address of his ex-wife. With this information and the credit reporting agency's file,⁵⁹ the bank conducted its own investigation. It contacted the FBI,⁶⁰ whose files also showed the conviction.

Smith has two remedies: he may seek expungement of his criminal record or sue the VA under the Privacy Act.⁶¹ Expungement is generally available only when there is either an acquittal or dismissal of the charges and a showing of "significant abuse of authority" by the law enforcement officials.⁶² Expungements have also been ordered in cases where the sole purpose of an arrest was to harass civil rights workers.⁶³ A suit to obtain expungement, however, is uncertain and time consuming. A better option is to seek a remedy under the Privacy Act.⁶⁴ If the VA refuses to amend his military record, Smith may seek compulsion of such action through the courts.⁶⁵ The VA can argue that it is exempt from the requirements of the Privacy Act because its disclosure to the bank was a "routine use" of such records.⁶⁶ Smith undoubtedly signed a waiver as part of his application for

58. *Id.* § 1681(g). See also A. MILLER, *THE ASSAULT ON PRIVACY* 82 (1971); D. LIOWES, *Are New Privacy Laws Needed?*, 44 *VITAL SPEECHES OF THE DAY* 436 (1978).

59. 5 U.S.C. § 552a(b) (1976). If the bank already had this information, it could have notified the VA, whose activities are excluded from the provisions of the Right of Financial Privacy Act under the circumstances described here. *Id.*

60. *Id.* The FBI's activities are also excluded under these circumstances.

61. 5 U.S.C. § 552a (1976).

62. See, e.g., *Menard v. Saxbe*, 498 F.2d 1017 (D.C. Cir. 1974); D. WEINSTEIN, *Confidentiality of Criminal Records: Privacy v. the Public Interest*, 22 *VILLANOVA L. REV.* 1205-11 (1977), points out that data collection, not just computerization, is at least part of the problem. The criminal justice system has a genuine need, however, for data to prevent crime, move caseloads, and analyze statistics.

63. *United States v. McLeod*, 385 F.2d 734 (5th Cir. 1967).

64. 5 U.S.C. § 552a (1976).

65. See *id.* § 552a(g)(2)(A).

66. See *id.* § 552. The term "routine use" means, with respect to the

the mortgage guarantee, permitting the bank and the VA to investigate his record and use any information they received. Any information disclosed under the Privacy Act must be "timely"⁶⁷ and Smith's seventeen-year-old conviction does not meet this requirement.

Smith's available remedies do not necessarily provide certainty of outcome and the process required to pursue these remedies is extremely time-consuming. As a practical matter, the house Smith sought to purchase would probably be sold to another bidder. His best non-legal remedy may be to seek a conventional loan from another bank using a different credit reporting agency.

Mary Brown, a thirty-year-old television reporter in perfect health and with an excellent financial reputation, was informed that she would not be issued an insurance policy. The insurance company notified Brown that it had received adverse information about her that she could inspect. At the insurance company's office Brown was shown her file with the exception of her medical and credit reports.⁶⁸ She was, however, given the names of the credit reporting agency and the doctors the company had contacted for this information. The insurance company told Brown that it had received an adverse report from the Medical Information Bureau (MIB),⁶⁹ and that this report had been used to supplement the credit and medical reports.

The MIB, which is subject to the requirements of the Fair Credit Reporting Act,⁷⁰ was required to show Brown her file, excluding medical information. The file contained a report from a neighbor who stated that Brown entertained people of questionable character at all hours and that she used drugs.⁷¹ Brown disputed the report and the insurance company reinvestigated. It found that the neighbor was nearly senile and disliked Brown because her dog occasionally wandered into the neighbor's yard. The insurance company deleted the report.

The file of the credit reporting agency contained no adverse comments. The doctor's report, however, indicated that Brown had disclosed to her col-

67. *Id.* § 552a(e)(6). The Fair Credit Reporting Act does not permit disclosures of convictions over seven years old.

68. Although this is an accepted industry practice, routine medical information, such as a blood pressure reading, may be disclosed to the individual. *Id.* § 552a(f)(4).

69. See Stern, *Medical Information Bureau: The Life Insurer's Databank*, 4 RUTGERS L.J. OF COMPUTERS AND THE L. 1, 1-19 (1974). The MIB is an association of 700 life insurance companies whose members underwrite 90% of the life insurance policies in the United States and Canada. Members may obtain information on the records of over 11,000,000 people contained in the MIB's computer files. Whenever an applicant is declined life insurance, the life insurance company reports this information to the MIB. This list is not checked for accuracy and the person is placed on a list of "impairments." The traits of an "impairment" include nervousness, sexual deviation, and unhealthy appearance. The purpose of the MIB is to prevent an applicant who is a poor risk and who is refused insurance by one company from applying to subsequent companies or from withholding certain information. While the MIB will not divulge such medical information directly to an applicant, it will provide information to the applicant's personal physician, who may then inform the applicant. Under the MIB rules, such medical information is to be used only to supplement the life insurance company investigation. *Id.*

lege physician that her mother had been treated by a psychiatrist.⁷² The college was precluded from releasing this information under the Family Educational Rights and Privacy Act (Act)⁷³ without Brown's consent. This Act, however, does not provide a private remedy; it merely permits the Secretary of Education to terminate federal funds to the institution.⁷⁴ Brown does have a remedy against the credit reporting agency for continuing to carry the doctor's report. The agency is precluded from disclosing the information because it is more than seven years old.⁷⁵ If the agency refuses to both delete the information and inform the insurance company of this action, the agency may be liable for actual and punitive damages.⁷⁶ If the agency changes its report, Brown should be issued her policy.

Richard White, a forty-year-old small businessman who owns his own hardware store, was denied a credit card. The credit card company showed White his file, with the exception of his credit report, and gave him the name of the credit reporting agency. The file at the credit reporting agency revealed that shortly after graduating from college twenty years ago, White was adjudicated as bankrupt and received welfare for a year.

Under the terms of the Fair Credit Reporting Act, bankruptcies that occurred over ten years prior to a report may not be disclosed.⁷⁷ The agency is required to delete the information and inform the credit card company or be subject to actual and punitive damages.⁷⁸ Other types of adverse information may be subject to a seven-year limitation on disclosure.⁷⁹ The agency may not, therefore, report that White received public assistance.⁸⁰

The more interesting question is how the credit reporting agency obtained this information since these records are subject to strict requirements of confidentiality.⁸¹ It is possible that White's social security number was obtained when he received public assistance⁸² or when he applied for the

72. This is another actual case reported to the Privacy Commission in 1978. A young woman was refused employment as a public school teacher because she had reportedly told her school doctor her mother had once seen a psychiatrist. See Diamond, *How to Protect Your Privacy*, McCALL's, Feb. 1980, at 51.

73. 20 U.S.C. § 1232g(b)(i) (1976).

74. See, e.g., *Girardier v. Webster College*, 563 F.2d 1267, 1276 (8th Cir. 1977) (a former student could not use the Family Educational Rights and Privacy Act to force a college to release his transcript after he had defaulted on his National Defense Student Loan and was discharged in bankruptcy).

75. 15 U.S.C. § 1681c(a)(6) (1976).

76. *Id.* § 1681n.

77. *Id.* § 1681c(a)(1). The credit report is used in connection with a transaction or life insurance policy involving an amount in excess of \$49,999 or employment at a salary of \$20,000 or more. There are no time restrictions placed on reporting bankruptcies.

78. *Id.* § 1681c.

79. *Id.* § 1681c(2)-(6).

80. *Id.* U.S.C. § 1681c(a)(6).

81. 42 U.S.C. § 602(a)(9) (Supp. IV 1980). In Colorado, information on individuals who applied for public assistance since 1972 is in computer files. Printouts of these files contain a note that the recipient is responsible for the confidentiality of the files. See 6 Colorado Department of Social Services Manual, §§ 6.210-6.220 (effective June 1, 1983).

82. *Chambers v. Klein*, 419 F. Supp. 569 (D. N.J. 1976), *aff'd*, 563 F.2d 1000 (3d Cir. 1977).

credit card. A computer search for information based on White's social security number might reveal such information. In any case, the agency must delete this information from its files and notify the credit card company, which then has the discretion to issue a card based upon this changed information.⁸³

These three cases suggest the pervasive impact that computer storage and retrieval of personal information can have on an individual's life. The burden of correcting inaccurate information or deleting dated material rests most often with the individual rather than the agency. This is because in many computerized databanks the cost to delete data is significantly higher than the cost to store it perpetually.⁸⁴ The real threat to privacy, therefore, may not be the fact that computers can collect and store facts about individuals, but rather that inaccurate or dated information can be repeatedly used to evaluate the character, reputation, employability, or credit-worthiness of an individual. That person may never know what information was used in the evaluation or from where the information was derived.

III. LEGAL PROTECTION OF PRIVACY IN THE UNITED STATES

A. *The Judicial Response*

Although the word "privacy" does not appear in the text of the Constitution, in the mid-1900's the Court found that such a right could be implied from its various amendments. In *NAACP v. Alabama*,⁸⁵ the Court found a "vital relationship between the freedom to associate and privacy in one's associations,"⁸⁶ ruling that the "right of the [NAACP] members to pursue their lawful private interests . . . privately" was protected by the first and fourteenth amendments.⁸⁷

tion. Davis, *A Technologist's View of Privacy and Security in Automated Information Systems*, 4 *RUTGERS L.J. OF COMPUTERS AND THE L.* 264, 273 (1975).

83. Credit card companies are a major source of information on millions of individuals. To obtain a credit card, the applicant must provide a significant amount of financial, credit, and personal information. When he uses his card, information concerning items purchased, travel movements, and financial status are posted to his account. By 1976, Master Card had 40.6 million cardholders. N. PENNEY & D.I. BAKER, *THE LAW OF ELECTRONIC FUND TRANSFER SYSTEMS* § 1.01[3] (1980). Credit card companies such as American Express, VISA, and Master Card contain specific instructions on their applications that the information requested, and information from later transactions, will be used and exchanged by other companies. This information is then sold to generate further profits for the credit card companies. One startling example of how information can be used occurred when a laboratory which tested women for pregnancy, sold its list of pregnant women to a diaper service. The diaper service mailed advertisements to the names on the list. One husband learned of his wife's pregnancy from the cheerful greeting and congratulations on the cover of the advertisement. *See* Comment, *The Privacy Side of the Credit Card*, 23 *AM. U.L. REV.* 183, 187 (1973). In Denver, Colorado, banks seem to be concerned about protecting the confidentiality of their customers' files. Most banks keep only a customer's balance, available credit line, and the past few months' transactions on computer files. The rest of the customer's information is stored by month, not by name, on microfiche, which is stored under tight security in the bank's vault. Interview with Jack D. Molloy, Law Department of Colorado National Bankshares, Inc., in Denver, Colo. (Dec. 14, 1982).

84. Interview with James R. Young, Advisory Engineering Manager of Storage Technol-
ogy Corporation, Boulder, Colo. (Sept. 23, 1982).

In holding that a constitutional right of privacy exists, *Griswold v. Connecticut*⁸⁸ struck down a state statute that made it a crime to prescribe or use contraceptive devices.⁸⁹ Justice Douglas found a right of privacy emanating from the penumbras of the first, third, fourth, fifth, and ninth amendments.⁹⁰

The Court, however, has been reluctant to hold that a similar right to privacy exists for individuals in commercial settings. In 1976, the Court in *United States v. Miller*⁹¹ held that a bank depositor has no "reasonable expectation of privacy" as to copies of checks, financial statements, and other documents that the bank depositor had supplied to the bank.⁹² The Court reasoned that because such records were merely business records, rather than private papers, and because the depositor voluntarily revealed personal affairs to the bank by surrendering these records, he took the risk that this information might be conveyed to others.⁹³

In 1972, the Court in *Laird v. Tatum*⁹⁴ avoided the issue of whether the existence of a broad system of domestic surveillance by the United States Army "chilled" the first amendment rights of those who were the targets of such surveillance.⁹⁵ Information concerning the activities of the plaintiffs in this class action had been stored in a computer at Fort Holabird, Maryland.⁹⁶ This information was freely disseminated to numerous military and civilian intelligence officials throughout the country.⁹⁷ The Court's holding was limited to a finding that the mere existence of broad governmental investigative and data-gathering activities was insufficient to constitute a justiciable claim.⁹⁸ Writing for the majority, Chief Justice Burger added that the ruling intimated "no view with respect to the propriety or desirability, from a policy standpoint, of the challenged activities . . ."⁹⁹ The dissent pointed out that danger exists as long as computer files are kept on the membership, ideology, and policies of any political activist group in the United States.¹⁰⁰

The latest Court decision dealing directly with this question of privacy occurred in 1977. In *Whalen v. Roe*,¹⁰¹ the Court held that as long as the security of the computer is adequate and the information stored therein is only passed to appropriate officials, sensitive information may be stored and

88. 381 U.S. 479 (1965).

89. *Id.* at 485.

90. *Id.* at 484. See also *Roe v. Wade*, 410 U.S. 113 (1973) (right of privacy includes the right to have an abortion); *Katz v. United States*, 389 U.S. 347 (1967) (overruling *Olmstead v. United States*, 277 U.S. 438 (1928)). *Katz* held that wiretaps without a warrant or the permission of at least one of the communicating parties was an illegal search, because the wiretap constituted an invasion of a reasonable expectation of privacy. 389 U.S. at 350-53.

91. 425 U.S. 435 (1976).

92. *Id.* at 442. See also *California Bankers Ass'n v. Shultz*, 416 U.S. 21 (1974).

93. 425 U.S. at 440-43.

94. 408 U.S. 1 (1972).

95. *Id.* at 3.

96. *Id.* at 6.

97. *Id.*

98. *Id.* at 10.

99. *Id.* at 15.

retrieved without an invasion of a person's right to privacy.¹⁰² Justice Stevens, writing for the majority, stated that the right to collect personal information "is typically accompanied" by a duty to avoid disclosure, and that the proper concern and duty were shown in this case.¹⁰³ Justice Brennan, concurred, recognizing that databanks increase the opportunity for abuse of privacy and that future developments in computer technology may necessitate a judicial curb on that technology.¹⁰⁴

Although a number of privacy and computer-related cases have arisen since *Whalen*, none have gone beyond the court of appeals level.¹⁰⁵ Consequently, the Court has yet to take up the issues foreseen by Justice Brennan.

B. *The Legislative Response: Federal Statutory Developments*

As a result of growing public concern about perceived abuses of privacy through computerized databanks and in response to the Supreme Court's reluctance to find constitutional violations of privacy in areas such as personal credit information, Congress enacted several statutes creating remedies for dealing with privacy violations.

1. Fair Credit Reporting Act of 1970

The first major legislation concerning credit data was the Fair Credit Reporting Act (Act).¹⁰⁶ The main provisions of the Act are intended to protect individuals from inaccurate reports and to prevent invasions of privacy.¹⁰⁷ The applicability of the Act is limited to reports for credit, employment, insurance, and related benefits.¹⁰⁸ To guard against inaccuracies, the Act gives the individual the right to access and to challenge data that a credit reporting agency may have in its data files. The statute also mandates procedural requirements for imposing civil penalties on credit reporting agencies if they fail to correct inaccurate information.¹⁰⁹ The Act allows the individual access to both the data and its source. If an individual is either completely or partially denied credit based on the credit report, the Act requires the creditor to disclose both the reason for the rejection and the

102. *Id.* at 601-02.

103. *Id.* at 605. Information in the databank included the names and addresses of everyone in New York who had acquired narcotic drugs such as opium and cocaine with a doctor's prescription. *Id.* at 591-93. The computer's security system included a locked wire fence, an alarm system, and off-line reading of the data files and tapes such that no computer terminal outside the computer could read or record the information. *Id.* at 594. The plaintiffs argued that the availability of their names and addresses from the databank created a concern that people in need of such drugs would refuse to seek medical assistance for fear of being discovered and stigmatized as drug addicts. *Id.* This argument was rejected. *Id.* at 603-04.

104. *Id.* at 607 (Brennan, J., concurring).

105. *See, e.g.*, *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570 (3d Cir. 1980); *Ash v. United States*, 608 F.2d 178 (5th Cir. 1979), *cert. denied*, 445 U.S. 965 (1980); *Doe v. Webster*, 606 F.2d 1226 (D.C. Cir. 1979); *United States v. Choate*, 576 F.2d 165 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978); *United States v. Roberto Benlizer*, 459 F. Supp. 614 (D.D.C. 1978).

106. 15 U.S.C. §§ 1681-1681t (1976).

107. *Id.* § 1681a.

108. *See* ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42,

name and address of the credit reporting agency.¹¹⁰

The Act requires that an individual be notified within six months that a credit report has been requested. The scope and nature of the request and the name of the creditor requesting the information must also be divulged.¹¹¹ Perhaps the most important provision in the Act gives an individual the right to challenge the accuracy of information contained in the credit reporting databank files.¹¹² As long as the challenge is neither frivolous nor irrelevant, the agency must reinvestigate and delete information found to be unverifiable. If the dispute is not resolved, the individual may file an account of the supposed inaccuracy with the credit reporting agency. This account must be included in all subsequent reports that the agency passes on to requesting creditors.

The Act also requires that reasonable procedures be followed by agencies in assuring the accuracy and proper use of credit information.¹¹³ If an agency is negligent in this area, an individual who is harmed may recover actual damages, costs, and attorney's fees.¹¹⁴ If the agency's action is willful, punitive damages may be awarded.¹¹⁵ Criminal penalties, including fines up to \$5,000 and/or imprisonment up to one year, may be rendered for the willful misappropriation or unauthorized disclosure of credit information.¹¹⁶ Federal courts have jurisdiction over violations without regard to the amount in controversy.¹¹⁷ To guard against invasion of an individual's privacy, the Act restricts the purposes for which credit reporting agencies may provide information. Proper uses include determining eligibility for additional credit and disclosure pursuant to a court order.¹¹⁸ Limitations are imposed on the length of time certain derogatory information may be retained by the credit reporting agency. For example, bankruptcy information can be retained only fourteen years.¹¹⁹ Arrest records, indictments, and convictions can be retained for only seven years.¹²⁰

The Act has certain weaknesses. It lacks a formal procedure to ensure that an individual be given due process and it provides a haphazard approach to deal with disputes about the accuracy of information in an individual's file.¹²¹ For example, objections and accounts by an individual in unresolved disputes concerning the accuracy of credit information are not reported retroactively to prior recipient-creditors of the individual's file. Further, the Act only mandates that a credit reporting agency provide the individual with an oral report of the contents of the credit files. The agency

110. *Id.* § 1681m.

111. *Id.* § 1681g.

112. *Id.* § 1681i.

113. *Id.* § 1681e.

114. *Id.* § 1681o.

115. *Id.* § 1681n.

116. *Id.* §§ 1681q-r.

117. *Id.* § 1681p.

118. *Id.* § 1681b.

119. *Id.* § 1681c.

120. *Id.*

need not provide the individual direct access or a written copy of the file.¹²² Finally, civil action remedies are difficult to obtain because the burden of proof is on the plaintiff-individual and it is often difficult to show actual monetary damages.¹²³

2. Privacy Act of 1974

The Privacy Act (Act)¹²⁴ supplemented the Freedom of Information Act¹²⁵ and was the second major piece of legislation dealing with privacy. The Act prohibits federal government offices from disclosing personal information about an individual without his written consent, unless it falls within one of eleven exceptions.¹²⁶ Restrictions on disclosures include not only hard copy, but also display and telephone transmissions.¹²⁷ The Act requires federal agencies to reveal their data-collection activities on individuals, to make their justifications for the collection and use of such data public, and to give individuals a right of access to the collected information.¹²⁸

The right of access permits the individual to inspect the information in the presence of a companion. He may request that corrections be made and, if the request is denied, may file a statement of disagreement.¹²⁹ The agency holding the information has ten days to respond to this statement. If the agency refuses to amend the information, the individual has thirty days in which to request a review of that refusal. If the review supports the agency's decision, the individual has the right to judicial review.¹³⁰ If the agency agrees to amend the file, it must notify those to whom the record has been disclosed.¹³¹ An agency is not required to maintain records of the entities to which disclosures have been made.

In regulating the release of information, the federal agency is required to disclose the name of the agency or authority requesting the information, to determine whether the request is voluntary or mandatory, and to determine the intended uses of the information.¹³² The agency must publish an annual notice of each record system it maintains. This notice must include: the name of the system, its location, categories of data files maintained, routine uses and users, storage policies, retrieval, access control, retention and disposal of data, procedures to notify individuals as to the existence of and

122. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 174.

123. *Id.* at 177.

124. 5 U.S.C. § 552 (1976 & Supp. IV 1980).

125. *See infra* notes 140-44 and accompanying text.

126. The exceptions under 5 U.S.C. § 552a(b) (1976) are: 1) to officers and employers of the agency in the performance of their duties; 2) when required by statute; 3) for routine use; (4) to the Census Bureau; 5) for statistical research; 6) to the National Archives; 7) for a civil or criminal law proceeding; 8) to protect an individual's health or safety; 9) to Congress; 10) to the Comptroller General; and 11) pursuant to court order.

127. *Id.*

128. *Id.*

129. *Id.*

requests for their files, and inspection and challenge procedures.¹³³

Individuals who believe that their rights have been violated and who have been denied relief from the offending agency may sue in federal court for injunctive relief and civil damages.¹³⁴ Damages for willful violations of the Act are limited to \$1000 plus attorney's fees. Criminal misdemeanor charges and fines of up to \$5000 can be imposed on agency employees for willful disclosure.¹³⁵

3. Family Educational Rights and Privacy Act

The Family Educational Rights and Privacy Act of 1974 (Act)¹³⁶ permits federal funds to be terminated to any institution of higher education that denies parents the right to inspect the educational records of their children.¹³⁷ The Act does not apply to confidential letters of recommendation; to financial statements concerning the parents of college students; or to a situation where a student has waived his or her rights in these matters.¹³⁸ The Act provides that funds will be denied to an institution that releases such records to persons other than: school officials "with a need to know," state or federal education officials, research organizations, or persons with a lawful subpoena.¹³⁹ Private remedies are not available to students or their parents.

4. Freedom of Information Act

The Freedom of Information Act (Act)¹⁴⁰ was intended to compel federal agencies to divulge various records, procedures, and statements of policy to those requesting such information. The Act requires each agency to publish in the Federal Register¹⁴¹ a description of the place and manner in which the public may obtain such information.¹⁴² Agencies are not required to disclose information which would: constitute a "clearly unwarranted invasion of personal privacy;" jeopardize national defense; impinge upon internal personnel rules; reveal confidential financial information, trade secrets, personnel or medical files, geological information, or agency memoranda; or reveal investigatory records that can be obtained only by a valid subpoena.¹⁴³ Persons who are refused inspection of federal records may sue to enjoin the agency from withholding the information and recover costs and attorney's fees.¹⁴⁴

133. *Id.*

134. *Id.*

135. *Id.* at 13.

136. 20 U.S.C. § 1232g (1976).

137. *Id.* § 1232g(f).

138. *Id.* § 1232g(a)(1)(B) (waivers may not be required for admission or receipt of financial aid).

139. 20 U.S.C. § 1232g(b) (1976 & Supp. IV 1980). *See also* Girardier v. Webster College, 563 F.2d 1267, 1276-77 (8th Cir. 1977).

140. 5 U.S.C. § 552 (1976 & Supp. IV 1980).

141. *Id.*

142. *Id.*

143. *Id.* *See also* *id.* § 552(a) and Rose v. Dep't of the Air Force, 425 U.S. 352 (1976).

144. 5 U.S.C. § 552(a) (1976 & Supp. IV 1980). *See also* Mervin v. Bonfanti, 410 F. Supp. 1205 (D.D.C. 1976).

5. Tax Reform Act of 1976

The Internal Revenue Service is exempted from statutes that deny access to an individual's personal records held by third parties. The Tax Reform Act of 1976,¹⁴⁵ however, requires that a taxpayer be notified when records of his transactions are subpoenaed from a bank, credit reporting agency, or other party.¹⁴⁶

6. Right to Financial Privacy Act of 1978

The Right to Financial Privacy Act¹⁴⁷ was intended to restrict the federal government's access to financial records. In apparent response to *United States v. Miller*,¹⁴⁸ Congress imposed a duty of confidentiality on financial institutions.¹⁴⁹ Financial institutions often serve as creditors and their records are likely to contain credit reporting agency reports.

The federal government may be permitted access to such records by securing the written consent of the individual. Other methods include obtaining: a subpoena, a court order, or a search warrant.¹⁵⁰ Whenever the federal government seeks access to financial records, the individual must be notified.¹⁵¹ Governmental access may be challenged in every instance except those in which a search warrant was obtained. A civil remedy against the government or the financial institution is available.¹⁵² A fine of \$100 per violation, actual damages, court costs, and attorney's fees may be awarded. Punitive damages are available, if the violation was willful.¹⁵³

7. Fair Credit Billing Act

The Fair Credit Billing Act (Act)¹⁵⁴ enhances the protection that an individual has from inaccuracies in credit data. Detailed provisions exist for correcting billing errors.¹⁵⁵ The Act establishes a procedure for an obligor to identify his or her account, register the alleged error, and state the reasons for believing that an error exists.¹⁵⁶ The creditor has thirty days in which to respond.¹⁵⁷ Upon receiving notice from the obligor that an error might exist, the creditor may not issue an adverse report concerning the obligor's credit.¹⁵⁸

145. Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1525 (codified in scattered sections of 26 U.S.C.).

146. 26 U.S.C. § 7609(a) (1976 & Supp. IV 1980).

147. 12 U.S.C. §§ 3401-3422 (1976 & Supp. IV 1980).

148. 425 U.S. 435 (1976). See *supra* note 91 and accompanying text.

149. H.R. REP. NO. 1383, 95th Cong., 2d Sess. 7, reprinted in 1978 U.S. CODE CONG. & AD. NEWS 9273, 9305-06.

150. 12 U.S.C. §§ 3406-3409 (1976 & Supp. IV 1980).

151. *Id.* § 3405.

152. *Id.* § 3417.

153. *Id.*

154. 15 U.S.C. § 1666 (1976).

155. *Id.* § 1666(a).

156. *Id.*

157. *Id.*

8. Federal Reports Act

Section 3508 of the Federal Reports Act¹⁵⁹ restricts the exchange of information between federal agencies and imposes penalties for unauthorized disclosures.¹⁶⁰ When the agency seeks to acquire confidential information on an individual, its justification defense is limited by the Act.¹⁶¹

C. State Legislation

Supreme Court policy has generally been to allow individual states to define privacy rights. In *Katz v. United States*,¹⁶² the Court held that: "[P]rotection of a person's *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States."¹⁶³

At the state level, legal protection afforded privacy remains limited, inconsistent, and fragmented. Only ten states have provisions in their constitutions, which expressly protect privacy.¹⁶⁴ Seven of these states confer more limited recognition on the privacy right by closely associating it with the prohibition against unreasonable searches and seizures.¹⁶⁵ Florida, for example, extends protection "against the unreasonable interception of private communications by any means."¹⁶⁶ The Illinois, Hawaii, Louisiana, and South Carolina privacy provisions are broader, protecting against "invasions of privacy."¹⁶⁷ Washington and Arizona have narrower privacy provisions, which serve as the functional equivalent of the prohibition against illegal searches and seizures.¹⁶⁸

Privacy in the state context is also protected through judicial interpretation. Some state courts have imported a limited constitutional right of privacy into general provisions of their respective state constitutions.¹⁶⁹ Some of these states later inserted an express privacy provision into the appropriate section of their constitutions through legislation.¹⁷⁰ While the notion of privacy is a relatively new area for the United States Supreme Court, it is even newer to the states. With the exceptions of Arizona and Washington, the right of privacy has been included in state constitutions only since 1968.

159. 44 U.S.C. § 3501 (1976 & Supp. IV 1980).

160. *Id.* § 3508(b).

161. *See* *United States v. Davey*, 426 F.2d 842 (2d Cir. 1970).

162. 389 U.S. 347 (1967).

163. *Id.* at 350-51 (emphasis in original).

164. ALA. CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. § 12; FLA. CONST. art. I, § 12; HAWAII CONST. art. I, § 5; ILL. CONST. art. I, §§ 6, 12; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7. For an excellent discussion of state legislation in the privacy area and a full text of each state's statutes, see Cope, *Toward a Right of Privacy as a Matter of Constitutional Law*, 5 FLA. ST. U.L. REV. 631 (1977).

165. *Id.* at 636.

166. FLA. CONST. art. I, § 12. *See* Cope, *supra* note 164, at 637.

167. *See* Cope, *supra* note 164, at 637.

168. *Id.*

169. *See* *Breese v. Smith*, 501 P.2d 159 (Ala. 1972) (right to be let alone concerning hair length); *Melvin v. Reid*, 297 P. 91 (Cal. Dist. Ct. App. 1931) (invasion of privacy tort); *Cason v. Baskin*, 20 So. 2d 243 (Fla. 1944) (invasion of privacy tort).

170. Alaska, California, and Florida adopted privacy provisions subsequent to the dates of the court decisions discussed *supra* note 169.

State constitutional privacy provisions add another degree of protection against such devices as computer databanks.

The experience of the states suggests that the most effective means of protecting privacy is the adoption of a "package" of privacy measures in state constitutions. One commentator argues that three elements are essential in such a package. The first is the inclusion of a provision relating to the interception of communication. This provision is normally within the section on searches and seizures. The second is a freestanding right of privacy, following the models of Alaska, California, and Montana, that protects against governmental intrusions. Finally, appropriate language should be included to assure that the courts and legislatures have a mandate to fashion remedies against intrusions by the private sector.¹⁷¹ A state's adoption of such a package would help protect an individual's privacy right across the spectrum of possible invasion, including those involving computer databanks. Most states, unfortunately, have not been very active in the privacy area. Colorado, for instance, has acted particularly slowly. Other than various restrictions on the dissemination of information concerning people who apply for welfare assistance, little Colorado privacy law exists.¹⁷²

IV. TRANSNATIONAL ASPECTS OF PRIVACY

A. *Transborder Data Flows*

The development of complex computer systems, with greatly enhanced data processing capabilities enabling vast quantities of data to be transmitted within seconds across national frontiers, has made it necessary to consider international privacy protection of personal data. Privacy protection laws have been, or will shortly be, introduced in approximately half of the Organization for Economic Cooperation and Development (OECD) countries to prevent violations of certain fundamental human rights.¹⁷³ The privacy rights having considerable bearing on international law include: unlawful storage of personal data, storage of inaccurate data, and abuse or unauthorized disclosure of such data.¹⁷⁴

While certain countries have enacted legislation aimed at protecting individual privacy, there is a danger that disparities in national legislation might hamper the international flow of appropriate and necessary personal data. Such data flows have increased significantly in recent years and are bound to grow with the continued widespread use of computer and telecom-

171. Cope, *supra* note 164, at 730-43.

172. *See* COLO. REV. STAT. § 26-1-114 (1982).

173. The OECD has 24 members: Australia, Austria, Belgium, Canada, Denmark, Finland, France, West Germany, Greece, Iceland, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Members who have introduced privacy protection laws are: Austria, Canada, Denmark, France, West Germany, Luxembourg, Norway, Sweden, and the United States. Belgium, Iceland, Netherlands, Spain, Switzerland, and United Kingdom have prepared draft bills. OECD, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1981).

174. *Id.* at 5.

munication technology.¹⁷⁵ Overly restrictive or disparate legal constraints could lead to serious disruptions in sectors of the international economy such as banking and insurance.¹⁷⁶

A recent report by the United States House of Representatives Committee on Governmental Operations outlines the issues in the international regulation of transborder data flows.¹⁷⁷ The difficulty of the problems involved can be observed from that report which noted, *inter alia*, the following kinds of situations: 1) a diversified consumer products company rented a house which straddled the border of two European countries to maintain the option of having computer tapes in the venue most expedient to management purposes;¹⁷⁸ 2) a German multinational corporation established a central personnel information system in Sweden for administration and planning. This system contained information concerning the family, nationality, and skills of its employees. Company officials were not permitted to export this information;¹⁷⁹ 3) a United States company complained that its wholly-owned subsidiary in Germany is required by German banking law to process totally within that country. Thus, the computer hardware, software, and operations must be located in Germany, thereby, excluding the economies of on-line processing from its Chicago data center.¹⁸⁰

These problems are due, in part, to individual nations passing disparate privacy protection laws to control what many argue is an inherently international commodity—information.¹⁸¹ According to Professor Nanda: “[International] law has been rather slow in responding to the ‘information revolution’—the development and application of technology in electronics and information processing, and application of technology in electronics, resulting in sophisticated computers, cable and two-way television, direct broadcast satellites, and the like.”¹⁸² Nanda argues, however, that a rush to pass laws limiting transborder data could upset the “balance between the needs and interests of society for free flow of information and of the individual for adequate safeguards of personal data and protection of privacy.”¹⁸³

Present legal norms primarily apply to issues that can be fixed to a definable geographic locus, where responsibility can be attached and jurisdiction can be established. Data transmission and storage do not follow formal geographic boundaries. Traditional legal approaches have, therefore, proven unsatisfactory to governments attempting to maintain control over personal computer databanks. A related problem is where responsibility lies

175. For a detailed discussion concerning transnational data flow regulation, see Patrick, *Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines*, 21 JURIMETRICS J. 405 (1981).

176. *Id.*

177. HOUSE COMM. ON GOVERNMENTAL OPERATIONS, INTERNATIONAL INFORMATION FLOW: FORGING A NEW FRAMEWORK, H.R. REP. NO. 1535, 96th Cong., 2d Sess. (1980).

178. *Id.* at 24.

179. *Id.* at 18.

180. *Id.* at 17.

181. Patrick, *supra* note 175, at 406.

182. Nanda, *The Communication Revolution and the Free Flow of Information in a Transnational Setting*, 30 AM. J. COMP. L. 411 (1982).

183. *Id.* at 412.

with respect to internal data networks and commercial timesharing services that operate across national borders. Four possible parties to whom responsibility may be attached in a fairly simple data communication transaction are: the originator of the data message, the telecommunications carrier, the data processor, and the recipient of the data.

Two major legal issues surround transnational data flows. The first concerns the instruments that governments must develop in order to know what computerized data exists. The second involves the legal framework that can be developed to assure that agreements among various public and private parties can be enforced to enable the continuous, uninterrupted flow of data vital to economic prosperity and national security.

Data flowing across borders is affected by two jurisdictions. As the internal laws of countries differ, the legal assessment of the data and its uses may also differ. The thrust of legislative efforts has been to regulate personal information. Some law exists for regulating telecommunications and economic information, however, regulation of transborder data flows is almost nonexistent.

A fairly common area to consider with respect to potential regulation is data throughflow. This involves transportation of information across a country without the data being used in that country. For instance, in transmitting data from Germany to the United States, data might be transmitted telephonically to London and then by satellite or undersea cable to the United States. England is a passive way-station in the data flow between Germany and the United States. Some data processing, however, may occur in London. One example is the creation of a temporary file for more efficient transmission. The data are not used in England and typically do not include information on English subjects. Consequently, there will rarely be any English privacy problems associated with this data throughflow. There may be little reason to restrict such throughflow with national legislation. In contrast, if Sweden were the throughflow country, Swedish law places restrictions on the creation of a machine-readable file.¹⁸⁴ Although the file is temporary, Swedish legislation governs.¹⁸⁵ The file could not be established without prior issuance of a license by the Swedish government.¹⁸⁶

A second area to consider in developing sound regulations is the use of foreign service bureaus where processing of data for use in one country takes place outside that country. The privacy issue is not involved with the nature of the data processed, but rather with the effect of the relevant national privacy legislation that governs where the data are processed.

A third area is the nature and extent of data collected in one country to be marketed in another country. Examples include information relating to subscriptions to foreign periodicals and foreign credit reporting for credit cards and other forms of credit. As the economies of different countries become more interrelated, the sharing of personal information by credit reporting agencies becomes increasingly significant. Many countries, particularly

184. Data Act of Sweden, 5 COMPUTER L. SERV. app. 9-5.2a, No. 2 (July 1, 1979).

185. *Id.* § 2.

186. *Id.*

those in Scandinavia, have severely restricted the use of data among credit reporting agencies in foreign countries.¹⁸⁷

A fourth area to consider is the growth of multinational corporations. When companies expand across national borders, a need for personal data to be transmitted across those boundaries arises. Companies engaged in international trade communicate commercial and personnel information between countries. Employees tend to be more concerned about privacy issues than suppliers or clients because of the nature of data stored in personnel files. Two approaches have been taken to restrict access to personnel data. Sweden requires a license to create and export personnel information.¹⁸⁸ Norway has incorporated data agreements and restrictions on access to personnel data into contracts between employees and management for local and multinational corporations.¹⁸⁹

Outside the personal data context, transnational data regulations constrain the movement of data across national borders. These constraints conflict with the administrative and technological programs of most multinational organizations.

A traditional tenet of national sovereignty has been the ability of a country to manage its economic and social activities. Telecommunications and computer technology have the potential of reducing the ability of a country to manage its internal activities. For example, Canada is concerned about the drain of computerized data to the United States, and its inability to control this drain effectively. According to the Canadian Minister of Science and Technology: "Transnational data flow has created the potential of growing dependence, rather than interdependence, and with it the dangers of loss of legitimate access to vital information and the danger that industrial and social development will be governed by decisions of interest groups residing in another country."¹⁹⁰ Similar concerns have been voiced in France, where the economic data bases used to develop monthly and quarterly forecasts of European economic trends are designed in the United States and disseminated in Europe via networks owned by American firms.

Many nations are attempting to protect their computer industries and job bases through privacy legislation aimed at gaining an economic advantage over other nations in the areas of computers and data processing. Stricter privacy legislation encourages the storage of information in computers within that country. Information processing is a field in which thousands of jobs could be lost to foreign nations. Developing viable national information industries with the necessary technical infrastructure must be considered by these nations in developing legislation.

Telecommunications falls within this area because each nation's laws and policies will affect the services telecommunications carriers offer. The

187. *Id.* § 11.

188. *Id.*

189. Norwegian Personal Data Registers Act, 5 COMPUTER L. SERV. app. 9-5.2a, No. 5, § 1 (May 18, 1977).

190. Address by J. Hugh Faulkner, Canadian Minister of Science and Technology, before the United Nations (Aug. 1977).

telecommunication rates and tariffs levied by governments will affect transborder data flows. Finally, the way in which telecommunication carriers view their role in new fields, such as electronic funds transfer, electronic mail, interactive home communications, and international data traffic monitoring, will also have a major affect on transborder data flows.

One reason for processing data in a specific country may be to obtain special protection for personal information. Personal data files could easily be placed outside the jurisdiction of the country in which the persons are located. Consequently, national authorities would need multi-party governmental agreements to obtain disclosure of a particular personal data file. Another reason for placing a data file under the jurisdiction of a foreign country having stricter privacy legislation is to encourage people to store privileged personal information. Consequently, the high privacy standards of a country will be associated with the high standards of the data company.

The most obvious reason for moving personal data files and processing to a foreign country is that more lenient privacy legislation may exist in that country. Such countries are known as "data havens" and represent a substantial problem with respect to transborder data flows. It is feared that national privacy legislation will be ineffective due to transborder "datadrains." This fear is well-placed, primarily because of the practical difficulties in attempting to control foreign data drains. For example, it is difficult to determine the legality of the use of merged data in files in a foreign country whose privacy laws allow such mergers but where the use takes place in a country whose laws do not allow for such mergers. This problem is a major threat to the establishment of effective international privacy legislation.

B. *Selected Examples of Foreign Privacy Legislation*

1. Canada

Protection of privacy has been incorporated into the Canadian Human Rights Act (Act).¹⁹¹ The Act requires annual publication of a catalogue identifying each federal information bank, the type of records contained, and their derivative uses.¹⁹² Exceptions to this requirement concern information on international relations, national security, federal-provincial relations, and law enforcement.¹⁹³ The act grants an individual the right to inspect records containing information about himself and to correct inaccurate information.¹⁹⁴ A member of the Canadian Human Rights Commission is designated a Privacy Commissioner in charge of receiving and investigating complaints arising under the Act.¹⁹⁵

British Columbia enacted a Privacy Act in 1968, creating a tort action for willful invasion of privacy.¹⁹⁶ Proof of damages is not required.¹⁹⁷ No

191. Act of July 14, 1977, ch. 33, 1976-77 Can. Stat. 887.

192. *Id.* § 51(1).

193. *Id.* §§ 53, 54.

194. *Id.* §§ 2(b), 52.

195. *Id.* § 58.

196. 5 B.C. REV. STAT. ch. 336 (1979). *See also* TASK FORCE, *supra* note 121, at 137.

other nation has enacted a privacy tort. The Privacy Act in the United States provides only a civil cause of action for damages.¹⁹⁸

Quebec enacted a Consumer Protection Act (Act)¹⁹⁹ in 1972. Sections forty-three and forty-six allow individuals to examine credit reports and register comments. The Act, however, has no provisions to ensure the accuracy of credit reports since it lacks specific requirements and procedures for correcting false information.

Saskatchewan enacted the Credit Reporting Agencies Act,²⁰⁰ which is penal in nature and regulates credit reporting agencies through licensing. The licensed agencies are governed by rules requiring: release of information, the recording of only certain data, disclosure to the individual, registration of disagreements, and informing recipients that certain facts have been disputed.²⁰¹

2. Sweden

The major privacy legislation in Sweden is the Data Act of 1973 (Act).²⁰² The Act prohibits computer databanks from holding personal information without the permission and supervision of the Swedish Data Inspection Board.²⁰³ The Board's regulations extend to: the type of data that may be collected, the design and technical equipment of the data systems, notice and access to the public, disclosure of information, storage of data, and security.²⁰⁴ Penal sanctions for negligent or willful violations of the Act include fines and imprisonment of up to one year.²⁰⁵ A two-year sentence may be imposed for unauthorized access or alteration of data, referred to as "data trespass."²⁰⁶ Civil liability for damages may result from inaccurate information.²⁰⁷

3. West Germany

West Germany's Data Protection Act²⁰⁸ subjects databanks to criminal sanctions for privacy violations.²⁰⁹ In 1976, the Federal Data Protection Law (FDPL) was enacted which regulates the type of information that may be stored, processed, and transmitted.²¹⁰ The FDPL bars use of certain confidential data.²¹¹ Data processing is protected when an individual consents

197. *Id.*

198. 42 U.S.C. § 2000a-6 (1976); O.E.C.D., POLICY ISSUES IN DATA PROTECTION AND PRIVACY 13 (1974).

199. Ch. 74, 1971 Que. Stat.

200. Ch. 23, 1972 Sask. Stat.

201. *Id.*

202. COMPUTER L. SERV., *supra* note 184.

203. *Id.*

204. *Id.* § 6.

205. *Id.* § 20.

206. *Id.*

207. *Id.* § 23.

208. Data Protection Act, 5 COMPUTER L. SERV. app. 9-5.2a (Oct. 7, 1970).

209. *Id.* at 6.

210. *Id.* at 5 COMPUTER L. SERV. app. 9-5.2a, No. 3 (Jan. 1, 1978).

211. *Id.* § 1.

or legal authorization exists concerning the data's use.²¹² Once a data file is created, the individual must, upon request, be provided with information on stored data concerning him.²¹³ Individual access is denied under the FDPL where it would prejudice the function of the data base.²¹⁴ Time limitations for the retention of data bases are not specified, but are determined by need.²¹⁵ The German law lacks a provision for notification of disputes between individuals and databanks. Individuals may, however, report their differences to the Data Protection Officer.²¹⁶

4. France

The French Data Processing, Files, and Liberties Law of 1978 (Law)²¹⁷ created a supervisory Commission to enforce and regulate implementation of the Law. An unusual provision is that databanks must disclose to the public their authorization, purpose, access rights, categories of information, and recipient organizations.²¹⁸ An individual's right of access is subject to a preliminary inquiry by the Commission, which determines the relevance and necessity of the disclosure.²¹⁹ If the Commission decides in favor of the individual, the databank must release a copy of the file.²²⁰ No provision exists, however, for resolving disputes between individuals and databanks.

5. Norway, Denmark, and Austria

The Norwegian Personal Data Registers Act²²¹ mandates the legal presumption of obsolescence of any unfavorable personal credit information more than five years old.²²² The Austrian Privacy Act of 1978²²³ requires databank users to correct or delete inaccurate or incomplete information on individuals.²²⁴ The burden of proving the accuracy of the information lies with the user, not the individual or databank.²²⁵ The Danish Private Registers Act²²⁶ requires that when a credit bureau discovers inaccurate information on an individual the bureau must: make the necessary corrections, notify the individual, and send corrected reports to those who have requested credit information within the past six months.²²⁷

The previous discussion illustrates that a number of nations have begun to realize the importance of protecting confidential, personal information.

212. *Id.* § 3.

213. *Id.* § 13.

214. *Id.*

215. *Id.* § 14.

216. *Id.* § 21.

217. France: Law No. 78-17, 5 *COMPUTER L. SERV.* app. 9-5.2a, No. 4 (Jan. 6, 1978).

218. *Id.* art. 22.

219. *Id.* art. 21.

220. *Id.*

221. *COMPUTER L. SERV.*, *supra* note 189.

222. *Id.* § 15.

223. 5 *COMPUTER L. SERV.* app. 9-5.2a, No. 8 (Oct. 18, 1978).

224. *Id.* § 11(1).

225. *Id.*

226. 5 *COMPUTER L. SERV.* app. 9-5.2a, No. 6 (June 8, 1978).

227. *Id.* § 14.

Their privacy laws suggest some basic principles that could be incorporated into privacy legislation in the United States.

V. POTENTIAL DEVELOPMENTS TO PROTECT PRIVACY

A. *Industry Self-Discipline*

Self-discipline by the computerized credit industry is one inexpensive control. By developing a professional code of ethics, credit reporting agencies could police themselves. The Code of Ethics for the Association of Credit Bureaus of Canada serves as a tool for self-discipline in the Canadian credit reporting industry.²²⁸ Disadvantages of the system are that no specific person or entity may be held accountable for breaches of the code and that no specific penalties or authority exist to ensure compliance. Enforcement of the code is based on "moral suasion."²²⁹

B. *Ombudsman*

An ombudsman does not have regulatory or legislative powers, however, he can recommend regulations and legislation. The ombudsman could report to Congress periodically and publicize adverse effects of data collection and invasions of privacy.²³⁰ Suggested functions of the ombudsman include: considering specific injuries from misuse of information; advising and commenting on potential databank development; researching data classification; adjudicating complaints; establishing professional standards; examining types of information stored and used; licensing databanks; requiring periodic reports on systems procedures by operators of databanks; and approving the interchange or collation of information between systems. The simplicity and low cost of the ombudsman approach makes it particularly attractive. The ombudsman could immediately respond to an individual's privacy concerns. One problem, however, is that the ombudsman does not review systemic problems. Instead, he concentrates on individual databanks and individual complaints. Also, there can be no investigation until a complaint has been made. Difficulties may also arise when the ombudsman lacks the technical expertise to analyze a problem.²³¹ The concept of the ombudsman has never been widely understood or accepted in the United States. Implementing such a system, therefore, could prove difficult.²³²

C. *Single Identification Number*

A single identification number (SIN) for all records and information on an individual could reduce the social harm caused by identification errors. A SIN system compiles and retrieves information quickly and cost-effectively. It would promote centralization of data which could facilitate imple-

228. See TASK FORCE, *supra* note 121, at 164.

229. *Id.*

230. *Id.* at 162. See also R. FREED, COMPUTERS AND LAW: A REFERENCE WORK 42 (1976).

231. See TASK FORCE, *supra* note 121, at 162.

232. See R. FREED, *supra* note 230, at 42.

mentation of other technical controls. Germany employs a SIN system.²³³ Under that system, if a person changes his residence only one agency is notified; other agencies are notified automatically. Sweden, Norway, Finland, and Denmark also have SIN systems.²³⁴ Sweden uses a ten digit number, which refers to an individual's birthdate, geographic location, and check number.²³⁵ Although there have been proposals for SIN systems in the United States and Canada; neither country has adopted one. A proposal in the United States to utilize social security numbers as the basis of a SIN system was abandoned in 1970.²³⁶

Opponents argue that SIN systems can be abused and result in the loss of anonymity.²³⁷ Other risks associated with personal data, particularly computerized credit information, may not be eliminated by a SIN system. By reducing the identification factors to a single number, the possibilities for mismatching information on an individual may be increased. Errors made with respect to the assignment of the SIN could result in the information on an individual being lost or destroyed.

D. *Centralized Databanks*

Centralized databanks serve a function similar to the SIN system. Centralization standardizes all records into one central intelligence system. Like the SIN, the centralized databank concept is attacked because of the potential for too much power and control. In an investigation by the House Special Subcommittee on Invasions of Privacy in 1966, the concern for misuse and control became paramount.²³⁸ Public discussions indicated the need for a system of safeguards through federal legislation which would include coding procedures, codes of conduct, and a system for data verifications. Centralized databanks might perpetuate facts without methods or provisions for updating the information. Another privacy consideration is the high probability of error that exists when data are collected from several sources.

E. *Open Access*

Open access provides a means of holding the databank and its personnel accountable.²³⁹ In Canada, an individual who disagrees with the information may insert statements into the file.²⁴⁰ Legal problems arise when someone other than the individual inspects the record, as in the case of minors or incompetents.²⁴¹ If access is extended to include sources and uses of the information, an undue burden might be placed on the custodian of the

233. TASK FORCE, *supra* note 121, at 86.

234. *Id.* at 87.

235. *Id.*

236. *Id.*

237. *Id.* at 85.

238. *Hearings Before the Special Subcomm. on Invasions of Privacy of the House Comm. on Governmental Operations*, 89th Cong., 2d Sess. (1966).

239. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 39.

240. TASK FORCE, *supra* note 121, at 155.

241. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 150.

data thereby increasing the difficulty of obtaining confidential information.²⁴² Costs in providing access present another problem. In 1972, the Younger Committee estimated that mailing a complete printout on every individual in the United States could cost around \$2 million plus postage.²⁴³ Reports including a full explanation of the codes could cost twice as much.²⁴⁴ The Fair Credit Reporting Act of 1970 allows databanks to charge an individual requesting access.²⁴⁵ It is ironic that such a request and the subsequent visit to the databank allows the databank to gather more information on the individual.²⁴⁶

F. *Systems Controls*

Given the massive yet inexpensive storage capacities, it may be more costly to delete or update data than to retain it. Limitations can be placed on the kind of data that may be collected.²⁴⁷ Guidelines concerning updating and deleting data can be implemented.²⁴⁸ Nevertheless, problems still arise concerning the accuracy of data. Factual mistakes should clearly be corrected. The issue, however, is complicated when accuracy is a question of context. For example, an accurate account of unpaid debts may present a biased view without an explanation for nonpayment. If a question of context arises, the individual should be permitted to file a personal accounting. This approach is used in Canada.²⁴⁹

Data must be protected while in storage. Unauthorized persons who gain access to the databank could pirate or alter the information. One method of protecting confidentiality is to keep logs of those who access the files. Passwords, authentication, and authorization provide additional safeguards. Controls restricting access to the machinery itself may be incorporated into the software program. Physical processing restrictions which revoke certain features of the computer system also protect stored data.

Data output or dissemination must be protected. Exchanges of information between databanks could be restricted to persons having a demonstrable "need to know" or a common connection with the primary purpose for which the data was collected.²⁵⁰ Other controls include: individual approval for data exchanges, approval when the data are used for unintended purposes, and regularly providing lists of exchanges to the individual.²⁵¹

G. *Computer Security*

Security is the technical means by which confidentiality is ensured.²⁵²

242. *Id.*

243. TASK FORCE, *supra* note 121, at 155.

244. *Id.*

245. 15 U.S.C. § 1681 (1976).

246. TASK FORCE, *supra* note 121, at 156.

247. *Id.* at 150.

248. *Id.* at 151.

249. *Id.*

250. *Id.* at 153.

251. *Id.*

252. *Id.*

Passwords, limited access, audit logs, physical security, limitations on data links, and automatic labeling of sensitive files are examples of computer security.²⁵³ The costs of protecting privacy within a computerized system are primarily in the area of computer security. The expenses include: analysis, design and implementation of the protective system, tests and validations, operation and maintenance, salaries of security personnel, and computer time and maintenance costs.²⁵⁴ Hardware security costs include key-cards, closed circuit television, and shielded transmission cables.²⁵⁵ Password and audit procedures are added cost factors.

One commentator suggests that safeguards may cost more in "management attention and psychic energy than in dollars."²⁵⁶ These costs should be regarded as insurance against privacy invasions. Provisions exist that charge security costs to the subjects of the data rather than to consumers of the information. Access mechanism expenses, for example, are imposed on the individual under the New York Fair Credit Reporting Act.²⁵⁷

H. *Cryptology*

Cryptology encompasses signal security and signal intelligence. Signal security involves keeping secret messages between computers such as telegrams, telephone conversations, and electronic messages. Messages may be put into secret form by code or cipher. Elements of the message can be scrambled or replaced by other elements. The receiver, knowing the key to the encryption, reverses the process to read the original message.

Signal intelligence involves extracting information from transmissions. These methods include intercepting messages which are in plain language, electronic impulses, and radio or radar transmissions. Cryptanalysis breaks the codes or ciphers. Cryptology makes it difficult to intercept messages passing over lines or by radio signal between users and computer databanks. As with general databank security measures, cryptology can restrict access to those having a right to the information. Costs may rise with the use of cryptology, however, further insurance against privacy intrusions would be provided.

VI. FUTURE LEGAL TRENDS TO PROTECT PRIVACY

A. *The United States*

Additional legal steps may be taken to ease the tension between the need for rapid availability of data and the desire to protect privacy rights.

253. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 244; TASK FORCE, *supra* note 121, at 103.

254. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 248.

255. *Id.* at 249.

256. R. FREED, *supra* note 230, at 45.

257. N.Y. GEN. BUS. LAW § 380e(e)(2) (McKinney Supp. 1981).

1. Constitutional Amendment and/or Federal Statutes

One commentator argues that a constitutional amendment and federal statutes are needed: to balance the interests between the need for data and privacy protections; to restrict access of outsiders to confidential information; and to provide stricter sanctions and penalties for improper dissemination of personal data.²⁵⁸ This commentator concludes that federal sanctions and protections must be implemented because only a nationwide system will effectively protect privacy rights.²⁵⁹

Reliance on state privacy protection systems "will be only as strong as the weakest state law."²⁶⁰ In implementing legislation, the following aspects should be considered: 1) limiting the type of data maintained, 2) controlling the collection and recording of data, 3) informing an individual of the existence of a file concerning him and disclosing names of persons who have seen the records, 4) automatically expunging obsolete data, 5) permitting access to records only on a "need to know" basis, 6) categorizing files as personal or statistical, 7) easing the obstacles to discovery and proof, 8) limiting access to on-site retrieval, and 9) restricting the exchange of personal information between government agencies.²⁶¹

Those believing that a general right of privacy could be established by constitutional amendment or federal statute, in effect, propose that courts be the primary mechanism to enforce privacy rights. An injured party, however, would still need to bring an action. Courts will not initiate actions against databanks allegedly violating statutes. In today's political climate, it is unlikely that a constitutional amendment to protect privacy could successfully be enacted.

2. Federal Control Agency

A federal agency could be established to supervise and control governmental acquisition, storage, and release of computerized information.²⁶² A "Data Processing and Management Office" could act as a watchdog over federal utilization of computerized data and impose sanctions for violations of privacy standards. If this agency were given authority to register and license data systems, conformance with privacy safeguards could then be a condition precedent to obtaining a license.²⁶³

3. State Control Agency

A state control agency could use licensing and registration to monitor credit reporting agencies. Granting a state agency broad powers could, however, endanger privacy by giving the state access to confidential data. The

258. *Halla, Raising the Databanks: A Developing Problem for Technologists and Lawyers*, 5 J. OF CONTEMP. L. 245, 264-65 (1978).

259. *Id.* at 265-66.

260. *Id.* at 264-65.

261. *Id.*

262. *See, e.g., Comment, Agency Access to Credit Bureau Files: Federal Invasion of Privacy?*, 12 B.C. INDUS. AND COMM. L. REV. 125 (1970).

263. *Id.* at 127.

agency could be given power to intercede in the event of a violation, but not the power to correct the situation.²⁶⁴ The advantages of the flexibility of such an agency might be outweighed by its potential heavy-handed effect.²⁶⁵ Many of the concerns about a state privacy protection system may also be applicable to a federally-mandated privacy protection system.

4. Code of Fair Information Practices

A model Code of Fair Information Practices was developed in 1976 by the Ombudsmen Committee on Privacy of the Association for Computing Machinery.²⁶⁶ The code does not distinguish between public and private sectors. The guidelines apply equally, although it may be more difficult to control the private sector. A privacy protection code would be a sound foundation upon which states could develop a system for personal privacy, maximizing the utility of the computerization of information while minimizing abuses.²⁶⁷

B. *Transnational Trends*

Governments recognize that information is a powerful resource with political, economic, social, and cultural dimensions. They are, therefore,

264. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, *supra* note 42, at 92.

265. TASK FORCE, *supra* note 121, at 160.

266. OMBUDSMEN COMM. ON PRIVACY, ASS'N FOR COMPUTING MACHINERY, PRIVACY, SECURITY, AND THE INFORMATION INDUSTRY 72-79 (1976).

267. The code contains the following recommendations:

1. There should be no information system containing personally identifiable data whose existence is unknown to the data subject;
2. Personally identifiable data should not be collected unless the information system is safeguarded by a level of security commensurate with the sensitivity of the information;
3. There must be a reasonable method for the individual to find out what information is stored on him or her and how that information is used;
4. There should be no disclosure of any personal information to any organization or individual until the data subject has given permission for the disclosure in writing. Such permission may be revoked by the individual at any time, and if it is not revoked, the permission shall expire automatically at the end of one year;
5. Personally identifiable information collected for one purpose shall not be used for any other purpose without the knowledge and consent of the data subject;
6. In the event of a demand made by means of a compulsory legal proceeding, a reasonable attempt should be made to contact the data subject and to advise him or her of the demand prior to such information being given to the authorities;
7. There must be a reasonable method for an individual to contest the accuracy and completeness, pertinence and necessity of the data; to have data corrected, amended, or expunged if it is inaccurate or dated; and to assure that when there is a disagreement about a correction or expungement, the individual's claim is noted and included in subsequent disclosures;
8. Any organization creating, maintaining, using, or disseminating confidential information must assure its reliability for intended use and take precautions to prevent misuse of such confidential information;
9. Before creating a databank containing confidential information, a study should be completed to demonstrate the necessity for the information system as well as the relevancy of the collected data to its intended use. The concept of "useful life" should also be addressed; and
10. An individual should have the right to have the personal information removed from any file if the organization maintaining it cannot show any legal, useful, specific, and productive purpose for maintaining it.

motivated to consider implementing control mechanisms to promote national interests in the area of privacy. Public and private collectors, users, processors, and transmitters of this information realize that such mechanisms can result in constraints and costs attaching to transnational data flows and can see to participate in these governmental decisions.

The OECD and Council of Europe have taken major initiatives toward establishing an international legal regime concerning transborder data flows.²⁶⁸ Recommendations from both organizations recognize the need to balance privacy protection and the free flow of information. In the opinion of one commentator, the most significant of the OECD principles is the Individual Participation Principle which:

recognizes the right of an individual to obtain confirmation regarding the existence of data pertaining to the individual; to have such data communicated to him or her within a reasonable time in a reasonable manner and intelligible form at a charge, if any, which is not excessive; to be given reasons for the denial of such request and the opportunity to challenge such denial; and to challenge data relating to the individual and have it erased, rectified, completed or amended if the challenge is successful.²⁶⁹

In 1980, the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.²⁷⁰ It was opened for signature at Strasbourg, Germany on January 28, 1981²⁷¹ and seeks to protect individual privacy while allowing for the free flow of data across frontiers. Unlike the nonbinding recommendations of the OECD Guidelines, legally enforceable rights are established in countries that become parties to the Convention.²⁷²

Third World nations are attempting to develop high technology computer industries and will eventually face transnational data flow issues.²⁷³ They will probably ask multinational corporations for assistance and access to databanks containing information on economic forecasting, marketing, and statistical research. These countries will play a more active role in decisions concerning international communications policies and data flows.

CONCLUSION

An international convention ensuring that privacy protections are maintained is necessary. Increasing interdependence among nations compels the development of binding agreements to govern information flows while ensuring protection of personal privacy. Without such protection, continued development and sharing of computer and telecommunication technology may not occur at a pace beneficial to all parties involved. Without

268. Nanda, *supra* note 182, at 422-24.

269. *Id.* at 423.

270. *Id.*

271. *Id.*

272. *Id.*

273. *Id.* at 422-24.

1983]

COMPUTERS AND PRIVACY

483

international protections. The abuses in areas of illegal data storage, inaccurate data transmissions, and unauthorized data disclosures could continue at an alarming rate.

Changing Times
April 1983

The high-tech threat to your privacy

If you think computers know a lot about you now, just wait. Prospects for the years ahead make the need for privacy safeguards increasingly urgent.

WELCOME to the world of the American consumer, circa 1990:

► That deck of credit cards you used to carry around in your wallet is a nuisance of the past, replaced by a single "smart" card. In its computer-chip memory resides easily retrievable data about your bank balance, your credit rating, even the status of your health insurance. Thus equipped, you have instant access to all manner of goods and services with little or no hassle.

► Thanks to computer-assisted hook-

ups with local stores and banks, your television set now serves as an in-home buying and banking tool. If you want to use it the old-fashioned way, your choice of what to watch at any given time is almost endless because a central computerized "library" lets you call up any of hundreds of programs ranging from religious services to adult movies. And, if you're so inclined, you can take advantage of frequent opportunities to register your opinions on political and social issues by pushing the prescribed buttons in

response to questions on the screen.

► Computerized correspondence has largely done away with paper-and-pencil letter writing. Instead, you use an electronic mail system to flash your messages practically anywhere in the world in an instant. You get your answer via your home computer or TV screen.

Futuristic? Hardly. The technology that makes all this possible already exists; it seems only a matter of time before such scenes are common.

It's a prospect that has a lot of people worried. In all likelihood the data on a smart card will be recorded and stored in a computer file so that a verification will be available for legal purposes. Each time you use your TV set to make a purchase or

A wealth of data about viewers' reactions to two-way cable TV programs winds up in this Warner Amex control room in Pittsburgh. A strict privacy code prohibits disclosure of such data by the company.



choose a program or register an opinion, a record will be made of it. Each time you send or receive an electronic letter, a record will be made of where it went and where it came from.

Records such as these can reveal a lot about your private affairs that you probably wouldn't want very many people to know. This is why many privacy experts, contemplating the potential misuse of the wealth of information being compiled on individuals, consider computers a more serious threat to privacy than any other technological development of the 20th century. However, they stress that if proper safeguards are included, protection and confidentiality are possible with computers.

The question boils down to this: What guarantees do private citizens have that these records won't be used against them by the businesses or government agencies that have access to them?

The threats to privacy

There are some federal and state laws already on the books to protect privacy, and some two-way television and computer companies have developed privacy codes of their own. But the collection and computerizing of personal information about you is proceeding at such a rapid rate that technological developments are rendering past protections obsolete.

Arthur Bushkin, who worked on privacy issues in the Carter administration and is now a Washington consultant, sees three major threats.

► **Eavesdropping.** Wiretapping and interception of private radio communications is generally prohibited by federal and state laws. Law enforcement agents, for example, usually cannot engage in wiretapping without a court order. But eavesdropping on radio communications has become easier with the development of sophisticated scanners.

► **Privacy of records.** This is Bushkin's principal area of concern. "The catalyst here is the computer and its magnificent ability to store and disseminate information," he says. Businesses, banks, governments and other institutions have been putting together fairly extensive records on all of us for a long time, but once records are fed into computers, it is possible

"We may soon be leaving a computerized trail not only of financial transactions but also of our movements and habits."

not only to compile more information faster but also to provide almost instant access to it by people unknown to us and for reasons never stated to us.

► **Surveillance.** "Computers," notes Bushkin, "can follow you around." We may soon be leaving a computerized trail not only of our financial transactions but also of our movements and habits. Credit-card transactions already leave a trail, and the smart card may reveal even more about you.

"During the next two decades," Bushkin predicts, "we will become a wired nation. We will have the inherent capability to build up a much broader profile of people's habits and track the location of behavior. This will force us to examine some very fundamental questions about the kind of society we are."

Computer systems offer great potential for law enforcement, Bushkin believes. It will probably be possible to program them to find someone who is on the FBI's ten-most-wanted list. "On the other hand," he asks, "do we want to use these systems to search for people with more than three outstanding parking tickets?"

Robert Ellis Smith, publisher of *Privacy Journal*, a monthly newsletter, fears that two-way television will create the major privacy problems of the future. Two-way television is a form of pay TV, he notes. The companies providing the programs and services must know when and how the systems are being used so that they can bill their customers. The by-product of the billings is a computerized record of household habits.

Two-way TV can also provide burglar and fire alarm services. But to activate some systems, you must tell the company providing the services that you are leaving your home, thus creating a record of your comings and goings.

Smith, author of *Privacy: How to Protect What's Left of It* (Doubleday),

is also concerned about the ability of two-way TV and smart cards to monitor consumers' behavior without their knowledge.

He cites a recent experiment in Pittsfield, Mass., where consumers—voluntarily, in this case—agreed to have their purchases recorded to see how they were responding to television advertising. The bar codes found on virtually all packaged goods make it easy to track purchases. In the Pittsfield experiment, purchases were measured through the use of consumer identity cards as well as the bar codes. Such experiments, Smith fears, could be duplicated by examining the records of smart card and TV purchases without consumers' knowledge.

Sizing up the safeguards

Warner Amex Cable Communications, which operates the two-way interactive cable television service QUBE in cities in Ohio and several other states, is sensitive to the privacy issue. The company's 11-point Code of Privacy states that Warner Amex "shall maintain adequate safeguards to ensure the physical security and confidentiality of any subscriber information." The code also provides that information about individual subscriber viewing or responses "will be kept strictly confidential unless publication is an inherent part of the service (e.g., announcing a game show prizewinner)" and that Warner Amex "will refuse requests to make any individual subscriber information available to government agencies in the absence of legal compulsion. . . . If requests for such information are made, Warner Amex will promptly notify the subscriber prior to responding if permitted to do so by law."

Warner Amex's code has been tested at least once, and the company has stuck by its pledge. When a movie theater operator in Columbus, Ohio, was accused of showing a pornographic film, he protested that the film had already been on the QUBE cable system in Columbus and asked the company for the names of the people who watched it. A judge ruled that Warner Amex need not provide individual names, but the company was ordered to make public the percentage of its subscribers that or-

dered the movie and presumably saw it as well.

On a broader scale, only three states—California, Illinois and Wisconsin—now have laws seeking to insure privacy for subscribers to cable systems and two-way TV. The provisions are similar to the Warner Amex code. In addition, the California law prohibits a cable system operator from using "any electronic device to record, transmit, or observe any events or listen to, record, or monitor any conversations which take place inside a subscriber's residence, workplace, or place of business, without obtaining the express written consent of the subscriber."

This section, which is similar to one in the Illinois law, is designed to protect people from abuse of systems that, in effect, listen in to homes in order to provide fire and security protection. One such system links a TV set to a computer monitor capable of electronically sweeping a household every seven seconds.

So far, the interest in privacy-protection laws on a national scale is practically nil in Washington. A report on privacy dangers was issued by a special presidential commission six years ago. Its recommendations have not been enacted by federal agencies or Congress. Congressional hearings will be held this spring on safeguards for the use of tax information.

Little more than a decade ago, in fact, proposals were made for a centralized federal computer list that would combine all the information the government had about an individual, from social security records to military service and even arrest records. The proposals, which were backed and pushed largely by law-enforcement agencies, never got serious consideration.

Today there is no longer any talk about centralizing information because computer techniques have advanced so quickly that one master file is unnecessary. The same purpose can be served by computer matching programs. Two or more tapes containing different kinds of information can be run through a computer and compared to discover which names or information appear on both lists.

Such matching of tapes is being performed to find people suspected of being welfare cheats and govern-

ment workers who have failed to pay their federal student loans, and to identify youths who have not registered with the Selective Service System. In the last case, the social security numbers of youths who reach registration age are checked against selective service and armed forces lists. If a name on the social security list is not on the selective service or armed forces lists, the government scores a "hit" and provides the Selective Service System with the name and address of that person.

What's legal?

Information gathered about all of us by the government is supposed to be used only for the purpose for which it is obtained. But the interpretation of laws and regulations differs, and new laws can be passed. The Privacy Act of 1974, which spells out the rules for government agencies, restricts the use and disclosure of information. However, the selective service matching program was specifically authorized by Congress, and federal guidelines have been revised to facilitate computer checking for welfare cheats and delinquent student loans and to leave more discretion to individual federal agencies.

Henry Geller, former head of the National Telecommunications and Information Administration, a federal agency within the Department of Commerce, contends that for sensitive information there must be "an expectation of confidentiality" of information obtained from individuals by the government or anyone else. The U.S. Postal Service and the Internal Revenue Service have generally good records of protecting the privacy of the mails and sensitive tax information, says Geller, who is now a Duke University professor.

People worried about computer-assisted invasions of privacy insist that they do not want to thwart the computer industry. Rather, they say they seek a balance between technological advancement and citizens' well-established right of privacy.

"What makes America unique," says Geller, "is its treatment of the individual, and that must include a guarantee of the right of privacy. It is a part of the quality of life. Privacy and the dignity of the individual go together." □

Your medical records. How private are they?

By Alec Dubro

There was a time when medical records consisted of a few hastily scribbled notes stuck in a dog-eared file folder and shoved into the bottom drawer of the family physician's desk. If not exactly superfluous, they were almost incidental to the practice of medicine. All the really important information about a patient — often beginning with his birth — was filed away in the physician's memory.

All that has changed drastically in the past 50 years. As medicine has become more sophisticated and special-

ized, and as the population has become ever more mobile, the need for complete medical records has increased significantly. Today, an individual's records can run to hundreds of pages and are likely to be found in several physicians' offices and hospitals as well as in electronic data banks. Until this year, however, the patient himself did not have an automatic right to see his own medical records. If he wished to obtain them, he generally had to hire an attorney and have the records subpoenaed.

When Assembly Bill 610 became effective on January 1, a five-year legislative battle to open medical records to the consumer came to an end. The bill, sponsored by former Assemblyman Howard Berman (since elected to Congress), allows an individual to obtain his records without using the services of an attorney. The new law says, "(E)very person having ultimate responsibility for decisions respecting his or her own health care also possesses a concomitant right of access to complete information respecting his or her condition and care provided." Health & S C §25250.

Four previous attempts to pass legislation granting consumers access to their medical records had been defeated, almost entirely as a result of concerted efforts by the California Medical Association and the California Hospital Association. The CMA



Illustration by Dick Cole

*Few documents contain more
intimate detail than
medical records*

Medical Records

argued that open records would inhibit the physician's freedom to speculate about a patient's condition without fear of legal retribution, and would thereby diminish the quality of medical care.

Barbara Holstead of the Institute for the Study of Medical Ethics, a group organized to lobby for open records, said of the CMA's successful opposition to an earlier bill, "They've fought the bill for two reasons: One, they've always done things their way, and two, they want to preserve the present paternalistic system of medicine."

But paternalistic medicine had had little popular support in recent years. A 1979 Harris poll ("Dimensions of Privacy") showed that 91 percent of Americans, including 64 percent of physicians, supported the idea of open medical records. Nevertheless, the CMA opposed AB 610 until the organization was successful in adding an amendment allowing physicians the option of providing summaries of a record, rather than the entire document.

Before passage of AB 610, the State Board of Medical Quality Assurance received 300 to 500 complaints annually about denial of access to medical records, principally by private physicians. "Since few consumers are even aware of the BMQA," says its executive director, Robert Roland, "I assume that these complaints were just the tip of the iceberg."

Other complaints found their way to the Department of Consumer Affairs in Sacramento. Consumer Liaison Officer Candis Cohen says she found three groups of people who wanted their medical records. "The first group were changing doctors. The second were people who simply wanted to take more responsibility for their own health care. And the third group were women involved in DES cases." Many women who took diethylstilbestrol during pregnancy say they have had difficulty obtaining their medical records, as have their daughters, who want to see their mothers' records because DES has been linked to increased risk of uterine cancer in women whose mothers took the drug. DES mothers and daughters have also complained of slipshod or non-existent record keeping, uncooperative physicians and instances of "missing" files.

Like some physicians, a number of hospital administrators have consistently opposed the idea of open records. The Chicago-based American Hospital Association currently states that medical re-

ords "are regarded as the property of the hospital."

An administrator for one of California's largest health care organizations, who asked not to be identified, says that he feels there is no good reason to allow patients access to their records. Aside from those with a legal claim against the hospital—who could get their records through an attorney—he says the only people who would want to see their records would be "paranoids, criminally minded people trying to finagle a disability claim, and curiosity seekers." Of the Berman bill, this administrator says, "It will be an annoyance or nuisance at best. It creates a huge editing task, and if summaries are done by a physician, the reasonable cost will be from \$50 to \$100 an hour."

On the other hand, William Petrick, general counsel for the Permanente Medical Group, California's largest physician group practice, says, "We have always attempted to satisfy patients who wished to see their records. We have suggested they make appointments with their physicians to discuss their records, and we will continue to do so after the Berman bill takes effect. There are some unclear passages in the new law, but we will abide by its intent. We have, in fact, prepared request forms and established fees for those who do want to review their records or have them copied."

The CMA argued that open records would diminish the quality of health care.

Some lawyers also question the wisdom of showing a patient his medical record. Oakland attorney Steven Kazan, who frequently represents plaintiffs in asbestosis cases, says, "There could be good reasons for patients wanting to see records, specifically if they are receiving bad health care. But I'm not sure that unlimited access to records is productive. What one has the right to, and what is best, are not necessarily the same thing."

Kaiser-Fremont pediatrician Bennett Coplan feels otherwise. "If a patient asks to see his chart," says Coplan, "it is destructive to the doctor-patient relationship to deny access. There is a danger of misinterpretation by the patient, of course, but that's why I'll guide the patient through the chart. As for the supposedly chilling effect open records have on a doctor's candid observations, a lot of those things doctors are now afraid to write shouldn't be written anyway. There are ways to describe conditions so that colleagues can

understand without resorting to value-laden conclusions."

Roland agrees. "Health care ought not to be run for the bureaucrats, but for the consumers," he says. "People have a right to examine their records; the reason why doesn't matter. It should be a necessary and acceptable cost for the doctors and the hospitals."

Perhaps the most solid evidence in support of open records was revealed in hearings conducted in the mid-1970s by the Privacy Protection Study Committee. According to the committee's 1977 report, "Not one witness was able to identify an instance where access to records had had an untoward effect on a patient's medical condition."

If access to medical records has been the consumer's most immediate concern, the issue of access by third parties has raised the hackles of civil libertarians as well as consumers. A number of committees of the American Civil Liberties Union have devoted themselves to shoring up laws which limit access by those other than the health care provider and consumer, but the law, alone, does not ensure the privacy of medical records.

San Francisco attorney Wes W. Wagon has handled a number of DES cases for the San Francisco firm of Hersh & Hersh. He notes that although the law limits what medical records can be subpoenaed in a medical case (the Confidentiality of Medical Information Act, CC §56 et seq), the health care practitioner usually complies with a subpoena, regardless of its validity.

"We had a case recently," he says, "where opposing counsel subpoenaed psychiatric records which we deemed to be wholly irrelevant to the case. By the time we found out and made the motion to quash, the subpoena service had the records, and they were viewed by counsel. Ultimately we did obtain the return of the records, but the burden was on us to prevent private records from being made public."

The majority of records in third-party hands are not those subpoenaed in legal proceedings, however, but those in possession of insurance carriers. Since at least three-quarters of all medical bills are paid for by either public or private insurance, a lot of medical records leave doctors' offices.

In the past, abuse of medical record privacy by insurance companies was not uncommon. Insurance carriers readily exchanged information on persons seeking to purchase new insurance. Moreover, the records themselves were frequently out of date. Beyond the reach of the consumer, the records in insurance companies' data bases were not updated

Alec Dubro is a free-lance writer and editor living in Berkeley.

Medical Records

as were records in doctors' offices. "It is entirely possible," says attorney Monica Schrade Weil, of the Southern California ACLU Medical Rights Committee, "that a condition—medical or psychological—could be cured, yet once recorded (could) remain in a data bank forever."

Two years ago, the Legislature passed a law based on the National Association of Insurance Commissioners model bill, which guarantees the consumer a modicum of privacy and the ability to check his insurance records and correct mistakes (Ins C §§791.01-.26).

"The bill provides the same protection to the consumer as does the (federal) Fair Credit Reporting Act in other areas," says one insurance company's in-house counsel. "Basically, our problem has been one of balance—how to protect the privacy of our clients, and how to satisfy our need to check on what we are paying for. This law also enumerates carefully under what circumstances the carrier can disclose information to other agencies. The insurance companies here have become more sophisticated about disclosure; they've been feeling the pressure of

media stories and punitive damage judgments."

A great deal of medical insurance is carried by public agencies, where there is an even greater risk of record disclosure. State and local governments frequently maintain comprehensive files on abortions, for instance, ostensibly for public health reasons. Such files have been known to wind up in the hands of anti-abortion groups.

Frequently, it is simply the fear that medical records may fall into the wrong hands that proves detrimental to health care. Under the state's Short-Doyle law (Welf & I C §§5600 et seq), anyone seeking psychotherapeutic counseling may use community clinics, which are regulated by county health departments. In Los Angeles County, computerization of medical records has resulted in the inclusion of intake information on Short-Doyle patients, many of whom are labeled "mentally disabled" for record-keeping purposes. Patients so categorized have complained that this terminology goes into county files and is ultimately available to numerous data workers.

Fears of breach of privacy are not unfounded. Missouri Senator Thomas Eagleton's vice-presidential aspirations were dashed in 1972 when his psychiatric records were leaked to the press, even though they were protected by law.

Where protective legislation is concerned, the health care consumer in California has been gaining ground. Recent laws not only give patients access to their records but also seek to protect those records from unscrupulous insurance investigators and overzealous law enforcement personnel. None of these protections, however, alters the fact that the number of medical record data bases continues to increase. And the records they contain include a great deal of very personal information. As the executive director of the American Medical Record Association told the federal Privacy Protection Study Committee, "A complete medical record may contain more intimate details about an individual than could be found in any single document." It is no wonder, then, that medical records will be the focus of continuing concern for both consumers and attorneys. □

TK 7885 E
CRS MAIN FILE COPY

S-83 11960

Privacy and Videotex Systems

Two-way services bring with them the potential for abuse

by Richard M. Neustadt and M. Anne Swanson

Midway through George Orwell's 1984, the hero meets an old man and asks him how "Big Brother" got started. Things began to go wrong, the old man answered, when someone invented two-way television.

Advances in telecommunications promise to bring all sorts of conveniences to our doorsteps. We'll be shopping, banking, and working from home. We'll have computer-controlled electronic mail, burglar and fire alarms, and medical alerts, among other things. But along with this array of new services and products comes a potential for abuse.

The possible threat to privacy that home video and computing services pose is beginning to worry some people. The growth of nationwide videotex systems, whether they operate over cable TV or telephone lines, presents two major causes for concern. First, companies that sell electronic information or provide transactional services such as home banking and shopping will be able to compile dossiers on their subscribers. This information could be misused. Second, the proliferation of electronic transfer of information raises new questions about wiretapping.

Data Collection and Disclosure

The current debate focuses on the collection and possible misuse of subscriber records. Most companies that provide videotex services generate files on subscriber behavior as a mat-

ter of course. For instance, if the system operator provides information and charges his customers on a per-page basis, then his computer must keep a record of every video page subscribers request, if the system is used for transactions such as shopping or banking at home, the retailer or financial institution must keep a record, and the cable or telephone system operator may want to keep its own record as protection against claims of error.

Most companies that provide videotex services generate files on subscriber behavior as a matter of course.

Of course, similar records have always been collected by banks, hospitals, insurance companies, and other institutions. But with videotex systems, more records are being collected in one place. Moreover, computer files are easier to obtain than original documents.

The concern about collection of records leads to another issue: the possible disclosure of private information on consumer behavior. System operators may want to sell this data to retailers, pollsters, direct mailers, or credit investigators. Such information is commercially valuable, as indicated by the similar active market in magazine subscription

lists.

The action of a theater owner in Columbus, Ohio—where Warner-Amex runs its interactive Qube service—is an example of data disclosure. The owner of the theater subpoenaed lists of people who had watched "adult" movies on cable TV in order to defend himself against obscenity charges for screening those movies in his theater.

Protecting Privacy

Without a law or service contract to the contrary, company records belong to the company that collects them, not to the subscriber. The United States Supreme Court established this principle in 1976 when it held that a consumer had no constitutionally protected interest in his bank records that would enable him to challenge their release to government officials.

In the last two years, however, a movement has taken wing to legislate protections for those records. California, Illinois, and Wisconsin have passed privacy laws, six other states are seriously considering such measures, and the U.S. Congress may well pass a privacy law next year. While most of these bills are aimed at cable TV, the Illinois law and several of the proposed bills also cover two-way services provided over telephone lines. In addition, most cable TV franchises issued in recent years include privacy rules.

9/2/80
© 1983 BY BYTE Publications Inc.

Byte July 1983 V. 8

The central aim of this legislation is to require the system operator to obtain the subscriber's consent before collecting information. In most cases, collection without consent is allowed only for purposes of billing, providing a service like at-home shopping, or protecting against unauthorized reception or other services.

The measures vary on specifics. The Wisconsin law goes so far as to require cable operators to offer subscribers a free on-off switch controlling the interactive service. Some of the pending bills require system operators to acquire liability insurance to cover any suits based on violation of their privacy provisions.

Many people in the videotex field feel that all this legislation is unnecessary. They argue that there has been no evidence of abuse and that system operators are hardly likely to offend their customers by invading their privacy. These companies make a strong argument that we should wait to set rules until we know more about

the market and the technology.

Legislation is beginning to look inevitable, however. And when it does pass, the biggest problem for the videotex industry will be the motley of state and local rules and the often ambiguous wording of laws. The differences from law to law would, for example, require the operator of a system serving several states to maintain separate databases and procedures for each state—a costly proposition.

Some companies providing interactive services see self-regulation as the best way to allay subscriber concerns and avoid a patchwork of conflicting rules. Two large cable firms—Warner-Amex and Cox—have issued codes of behavior regarding privacy. The National Cable Television Association and the Videotex Industry Association have formed groups to draft industry-wide guidelines. Meanwhile, there is increasing support for a uniform standard, set by Congress, to preempt state and local rules.

Interception

In the case of interactive systems, several kinds of interception are possible. An eavesdropper—or a law-enforcement agent—could put a physical tap on a telephone line or dial into a central computer that transmits messages and keeps records. A cable subscriber could use special equipment to listen on his cable and pick up signals addressed to or transmitted by other subscribers.

Federal law provides criminal sanctions against unauthorized interception of wire communications and regulates legal wiretapping by law-enforcement authorities. The law allows government agencies to wiretap, but only with a court order—which the courts are to grant sparingly—or, if national security is at issue, pursuant to an order from the Attorney General.

Unfortunately, the drafters of this law—who worked on it almost 15 years ago—did not anticipate advances in technology, and the law now has two large loopholes. First,

the law covers only "aural interception," so it does not seem to apply to eavesdropping on data and text transmissions, such as electronic mail. Second, the law defines "wire communications" as transmission provided by common carriers such as the telephone company—probably omitting most cable services.

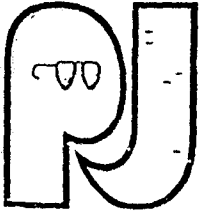
Legislation pending in Congress addresses both problems. Senate Bill 66 forbids any private person or government body from intercepting any broadband communication unless authorized to do so by the system operator, program originator, or federal law. (The provision does not specify whether law-enforcement investigators would use a regular search warrant or would have to meet the wiretapping law's strict standard to get court permission for nonaural interception.) This same proposal defines cable transmission as "wire communications" so as to include them within the law's scope.

It is too early to tell whether the privacy legislation pending in Congress will become law. If it does, it would preempt similar state regulation and would provide a unified substitute for the hodgepodge of different state and local rules. Although the federal proposal is currently part of a bill that focuses on cable systems, it is drafted broadly enough so that its provisions could be interpreted to include telephone-based services as well.

In the meantime, industry attempts at self-regulation on the privacy issue will increase. Most system operators are anxious not to scare their subscribers—it's hard enough to sell a new product without introducing fear into the equation. As a result, the Orwellian scenario may remain more fiction than fact. ■

About the Authors

Richard J. Neustadt is a partner in the law firm of Wiley, Johnson and Rein (1776 K St., NW, Washington, DC 20006). His recently published book, *The Birth of Electronic Publishing* (Knowledge Industry Publications, 1982), touches upon privacy and interactive video services. M. Anne Swanson is an associate with Wiley, Johnson and Rein.



PRIVACY JOURNAL

P.O. Box 8844
Washington, D.C. 20003
(202) 547-2865

an independent monthly on privacy in a computer age

September 1983, Vol. IX, No. 11

PROBING THE CAPITOL'S DRUG STORE

The Freedom of Information and Privacy Acts do not apply to the legislative branch, but some members of Congress may find their privacy diminished because of a court decision involving an anomaly on Capitol Hill.

There is in the Capitol an attending physician to tend to the aches and pains of members and staff. This is a Congressional office, but the physician's office gets its pharmaceutical drugs from the National Naval Medical Center, part of the executive branch. The current Congressional physician is a Navy admiral.

A persistent journalist named Irwin Arieff has requested under the Freedom of Information Act the list of prescription drugs that have been supplied by the Navy to members of Congress and Supreme Court justices over a six-year period. Arieff agreed that the Navy could delete any information that would possibly reveal particular individuals for whom a drug had been prescribed. The Navy refused his request, saying that even from cumulative information it would be possible to figure out what drugs were prescribed for particular individuals or at least for particular ailments.

The Court of Appeals for the District of Columbia, in a unanimous decision this summer, ruled that this "mere possibility" could not prevent the disclosure of the information Arieff is seeking. The court agreed with the journalist that the public has an interest in knowing the quantities of medicine dispensed without charge to Senators, Representatives, and others, as well as whether members are receiving drugs found to be ineffective by the Food and Drug Administration. Judge Antonin Scalia, a former University of Chicago law professor and Assistant Attorney General who is an expert in the Freedom of Information Act, found "justifiable concern" that some members of Congress will be victims of unfair speculation, but said he had no choice but to order the release of information unless there was an actual, not possible, invasion of privacy. Arieff v. Department of the Navy, 82-1536 (D.C. Cir. July 22, 1983).

The Department of Justice Civil Division routinely planned to ask the Court of Appeals for a rehearing, but this month asked the court for a 30-day extension in submitting its petition for rehearing "because a number of members of Congress have expressed concern" about the matter. In fact, according to the attorney handling the appeal, the concern came from the counsel for the Senate, a staff member.

Michael Davidson, the counsel, told PRIVACY JOURNAL that there had been no special concern raised since the court decision but that when the litigation began, the Secretary of the Senate and the Clerk of the House, both staffers, stated their concern to the Navy and asked the Navy to protect the interests of Congressional staff and members.

Now for your protection

A Computerized Prescription System at Giant Pharmacies

Giant's new computerized prescription system has many benefits for you and your family.

- Once you provide the information, Giant Pharmacists have your medical and drug history at their fingertips.
- The system warns of harmful effects a prescribed medication will have due to allergies or a medical condition.

- The system warns of harmful combinations of drugs. (Frequently, patients will see more than one doctor and neither doctor may be aware of what the other is prescribing.)

- The system can provide you with a complete record for insurance and tax purposes.

Available at all Washington Area Pharmacies



Consumer Medicine
Council Award
to Giant Food

"Please take a moment to fill out a registration form and take advantage of this added safeguard ... at no extra cost to you."

[From the New York Times, Nov. 20, 1983]

BIG BROTHER AND BLOCK MODELING

(By Scott A. Boorman and Paul R. Levitt)

As 1984 approaches, a quiet revolution in computers and information gathering may be bringing us closer than we realize to George Orwell's controlled state of Oceania. The public seems preoccupied with teen-age computer "hackers" accessing sensitive computer systems. But our more enduring fears should focus on a technology that corporations, nonprofit organizations and governments are using with increasing frequency to harness seemingly innocuous data from the personnel or communications departments and adapt it in new and unexpected ways such as targeting individuals for promotion or dismissal.

One name for this new computer game is block modeling—a programming technique that evaluates how employees fit within an organization on the basis of their relations with other employees. Recent impetus has come from such diverse independent quarters as Bell Laboratories, the American Broadcasting Companies, the Wharton School, and even the Institute for Social Management in Bulgaria.

Each of these organizations has recently spent time and money to develop advanced computer methods capable of "X-raying" a complex population—several hundred middle managers, for example—to detect structural patterns of interaction and communication. And though these technologies certainly have significant benevolent uses, their premise is a recognizable extension of the "guilt by association" idea, and can therefore be abused.

Most crucially, these methods have the capacity to capitalize on the unguarded moments of ordinary people; to probe organizations for factional alignments in a low-visibility and therefore insidious way; to play to human biases—particularly among managers—to name names; and to give sometimes facile technological rationales for settling complex personnel problems.

Block-modeling does not require particularly sensitive information like tax returns or medical histories. Rather, it exploits the unexpected, even uncanny synergy of large masses of "relational" data buried in organizational files. Examples of relevant data: Whom you talk with in your company; whose phone calls you do not return; whom you eat lunch with; whom you have worked with; who owes you favors; to whom do you send carbon copies of memos and letters; even whom you go bowling with. There is every expectation that far more such data bases will be routinely collected in the near future as minicomputer advances merger ever more widely with office information technology.

Only rarely will any relation between two people be very informative in isolation. But as many relations connecting many pairs of people accumulate, block modeling provides ways to distill frequently very striking and revealing patterns. Moreover, by throwing light on interlocking activities of specific people, block modeling goes a step beyond even the most refined kinds of geo-demographic data analysis such as extrapolating people's characteristics by Postal Zip Code of residence.

The output of a block-model analysis is simple to state—even deceptively so since a large amount of advanced mathematics and computing is involved. The block model of the social structure chops the social group up into "blocs." As Justice William O. Douglas once observed, a person is defined by the checks he writes. Blocs in block-modeling generalize this principle. They are discrete sets of people occupying similar positions in the relationship networks, and who are thus likely to behave similarly in ways important to the organization, and be candidates for receiving similar "treatment." Blocs can be, but don't have to be, tightly-knit groups or factions. Two people may never have heard of each other, yet can end up in the same bloc because of common patterns of relationship with third parties.

In the mid-1970's, we were part of a research team at Harvard that published the first papers on block-modeling's social applications. The response was revealing. Places like mental institutions and rehabilitation centers in Lithuania were quick to request reprints. Perhaps they saw block-modeling as a means to ferret out dissidents. Later, members of the group received inquiries from the Swiss as well as West Germans whose questions (and travel reports sent back home) were especially exhaustive.

Interest then seemed to wane until two or three years ago, when a wave of, if often unobtrusive interest started coming from American business sources.

Possible uses of block modeling, beyond deciding promotions and dismissals, could include the following:

Identifying sources of grassroots opposition in hostile corporate takeover situations or bankruptcy reorganizations.

Indicating where to put the "good stuff"—raises, promotions, funding, new employees and perks.

Obtaining early warning of trouble spots portending possible "blowups", in organizations, for example when internal tensions get out of hand, producing a wave of firings or resignations.

In fact, one of the earliest application of this class of methods was set in a Roman Catholic monastery which in the late 1960's was on the brink of organizational collapse. The block model successfully identified three factions—loyalists, "Young Turks," and outcasts—whose membership foreshadowed the way the organization would unravel. In an application to a more complex organization in difficulties, the block model not only correctly identified the outcast group, whose members would be dismissed, but also detected a submerged case of personnel misassignment in a different corner of the organization.

With proper safeguards, use of such methods can be sound, ethical and constructive. Obviously, internal audit departments should at times be permitted to scrutinize employees closely. But strides in the new "guilt-by-association" technologies are easily outstripping the vastly slower evolution of protective legal and administrative responses.

The typical employee whose position is likely to be most vulnerable to a block-model analysis is the middle manager, who has a family, a mortgage and a career locked into the XYZ Corporation. If the model locates him in a favorably regarded bloc, innocence by association prevails and all is well. But if he associated with known noncooperators, or, worse still, is assigned to a bloc judged likely to split off and found a rival company, he then can be passed over in the next promotion.

Inevitably, these new technologies create an unusually sensitive and complex web of management, privacy, information access, social control, and legal liability problems. In the end, the true 1984 threat lies not so much in the computer methods themselves, but in our society's slowness to react.

[From the New York Times, Nov. 27, 1983]

BLOCK MODELS AND SELF-DEFENSE

(By Scott A. Boorman and Paul R. Levitt)

Suppose you're an official of the Indianapolis chapter of a prominent national conservation group. Your organization's activities, along with those of 70 other diverse concerns, are being studied by a new computer programming technique called block modeling. This sophisticated technology studies your cash transactions, communications patterns and other recorded financial and social interactions. Unexpectedly, the computer says that your organization's financial and social profile is like that of the Ku Klux Klan; the John Birch Society; another environmental group; an emergency assistance association, and the American Legion.

You're all in the same "bloc," the computer says, the study is publicly available and the guilt-by-association consequences are all too obvious.

This example is real—part of a study recently reported in a scholarly book whose findings are impeccably qualified. It graphically illustrates possible problems created by block modeling—a powerful new information technology for classifying individuals and organizations based on large amounts of seemingly mundane data on transactions and relationships.

While the craft of block modeling is inaccessible to all but a few information "elite," its powers have not been lost on highly placed individuals in foreign and domestic corporations, as well as nonprofit organizations and government agencies. Those who use block models exploit them as an efficient way to sort the good from the bad from the indifferent—whether people, programs, divisions or rival groups.

Applications of block modeling and sister technologies already number in the hundreds. Block modeling is coming of age and possible applications include management (separating fast-track from slow-track employees), banking (studying electronic funds transfers and other cash flow patterns), professional sports (figuring out the pro draft), law enforcement (investigating conspiracies) among others.

But despite the versatility and broad appeal, genuine problems can arise. Computer-generated classifications have a strong mystique. And it can be hard indeed to fight a computer classification whose hallmark is naming names through a computer analysis of ordinary activities.

The classification problems truly come to the fore in the national political arena. For example, a study of Washington special interest groups has been using a kin-

dred method to probe similarities among more than 70 organizations on the basis of shared "issue interests" in health-related areas like Medicare and abortion. The resulting computer diagram lumps the Environmental Defense Fund with the American College of Cardiology and Merck & Company in a location far removed from major labor organizations like the United Auto Workers and the A.F.L.-C.I.O. One need not be a lobbyist or P.A.C. specialist to sense some of the political electricity of this placement, or possible action implications.

But what defense does an organization or employee have against the possible misuse of block modeling or sister methods. One should not look to Congress to pass a law. Waiting for legislation is like waiting for Godot. One should also not expect easy recourse through the traditional civil lawsuit. In fact, the law has yet to define limits to the block modeling enterprise and little legal fault can currently be found with most of the means of gathering the needed information for its use.

Still, protective rules need to be fashioned, even if they must sometimes fit in the nooks and crannies of legal categories—a new clause in a union contract for example. In most situations, an employee should at least be notified if he is the subject of something like a block model analysis by his employer. If you are an unsuspecting victim, there is no way to defend yourself. Then, focusing on rules for employee protection, a range of unique problems must be dealt with.

For example, the thrust of early computer-oriented privacy legislation from the 70's was giving people the right to examine information in their own "files." The privacy gains were genuine, but from a standpoint of block modeling, they are largely irrelevant. That is because block modeling classifies people on the basis of where they fit in a far larger web of relationships.

Therefore, one has to be concerned with many more "files" than just one's own—some belonging to people one has no direct connections with. One is thus vulnerable to all the problems of these third parties, including inaccuracies in their files. But if the third parties' privacy rights are to be respected, much of this relevant information must remain inviolate.

Thus, individuals being classified through a block model or similar method need to be given a carefully calibrated set of rights to information in order to interpret their assigned positions and respond accordingly.

This information should at least include some basic knowledge about the data base, including the scope of the population being modeled as well as what specific types of data have been, or will be, included.

Such data gives a crucial basis for understanding one's recourse. For example, if the block model put you in an unfavorable category, and used such data as whom you bowled with or went to parties with, this use of non-job related information could be attacked as gratuitous.

One might contemplate giving an employee access to the full data base stripped of personal identifying information except his own location in it. However, the wide availability of precisely such tools as block modeling makes recovery of identities from even such apparently "stripped" files a real privacy risk.

Still, one may disclose the structural role of the different blocs without dipping down to a level of individual identities. This last type of information, combined with a specific right to know your individual bloc location, can be enough to give a respectable road map for defense against the worst implications of guilt by association. Very importantly, effective ways also need to be developed to permit members of the same block to get together to mount a common defense. In contrast to abuses like "redlining" or race, sex, or age discrimination, the new technologies frequently pick out less than obvious groups whose members may easily fail to recognize they are being targeted in common.

Currently, technical progress in block modeling is making it possible to conduct an aggressive defense by showing that in some cases there is an equally good block model leading to very different classifications. In other words, there's more than one way to structure the given data—so that one block model might, for example, stress conflicting factions while a second identifies options for negotiation or cooperation.

Thus, responsible users of block modeling methods should also be prepared to disclose major alternative ways of organizing the data.

In the meantime, possibly the most important 1984 New Year's resolution is to remember that each time you pick up the telephone or send electronic mail in your office, you may be adding to somebody's computer data base—and computers never forget.

**DOCUMENTARY IDENTIFICATION AND MASS SURVEILLANCE
IN THE UNITED STATES***

JAMES B. RULE

State University of New York, Stony Brook

DOUGLAS McADAM

University of Arizona

LINDA STEARNS

Louisiana State University

DAVID UGLOW

DCI Research Associates

Reliance on documentary identification such as computer records, identification cards, and official papers is an essential feature of life in today's advanced industrial societies. This paper examines the history and use of six of the most common personal documents in the United States: Social Security cards, driver's licenses, credit cards, birth certificates, passports, and bank books. The increasing use and importance of such documents reflects the growth of new relationships between individuals and large, centralized organizations. These new relationships entail mass surveillance and social control, and result in increasing demands by organizations for personal data. We look at the strengths and weaknesses of these surveillance systems and the prospects of still greater social control in the future.

A distinctive feature of advanced industrial societies is the importance of personal documentation in relations between individuals and organizations. By personal documentation we mean two things: (1) the identification cards, certifications, licenses, and other organizationally generated tokens of identity held by private individuals; and (2) the data on persons developed by organizations and stored in computers or files for use in dealing with these people. These two forms of personal documentation usually work together: issuance or use of the first requires creation of, or recourse to, the second. Together, the two structure ongoing exchanges of information between persons and organizations which, we argue, bear importantly on the interests of both parties. Many social scientists have studied these exchanges and expressed concern about their effects upon individual privacy and autonomy (Rule, 1974; Rule *et al.*, 1980; Shils, 1975; Westin, 1967; Westin and Baker, 1972; Wheeler, 1969).

Social scientists are not the only ones to note the growing impact of personal documentation. It is practically impossible for an adult to live in the United States without frequent recourse to such things. One finding of our research underscores this fact: in 1976 and 1977 we surveyed 192 randomly selected households in Brookhaven Town, New York, and found an average of 28.8 different kinds of personal documents per household. The documents most often reported were Social Security cards, insurance policies, driver's licenses, birth certificates, personal checks, insurance payment records, marriage licenses, insurance identification cards, bank statements, tax returns, and savings passbooks. Social Security cards, the most widely held of these, were reported in 98 percent of the households; savings passbooks, the least widely held, were reported in 87 percent. When documents such as these are lost or accidentally destroyed, the resulting in-

* The authors thank the National Science Foundation, Division of Math and Computer Science, for a research grant (MCS 7700119), scores of conscientious interviewees for patiently providing data, and many Stony Brook colleagues and others for their comments. Correspondence to: Rule, Department of Sociology, State University of New York, Stony Brook, NY 11794.

convenience dramatizes the importance of the documentary link between the individual and the relevant organizations.

This paper presents a study of six of the most widely held personal documents in the United States: birth certificates, driver's licenses, Social Security cards, passports, bank books, and bank-issued credit cards. Each of these documents marks some kind of ongoing relationship between the individual holding them and the organization relying on them. Normally these relations entail complex claims and responsibilities between the two parties — claims and responsibilities specified and governed at least partly by information from the written or computerized records. Many aspects of these relations involve what we call *mass surveillance* and *social control* (Rule *et al.*, 1980).

By surveillance we mean any systematic attention to a person's life aimed at exerting influence over it. By social control we mean efforts to define and bring about "correct" actions or statuses. Surveillance and social control are ubiquitous social processes, but our concern here lies with their *mass* forms — that is, surveillance and control by organizations over large, otherwise anonymous publics. Such relations need not be malevolent or disadvantageous to the latter. A preventive health care system entails surveillance and control just as much as a system of political repression. Mass surveillance and social control, moreover, are often just two aspects of much more multifarious relationships between individuals and organizations — as indeed is the case in the six personal documents we studied.

There are two kinds of social control processes involved in these six personal documents. First, they enable organizations to exclude "inappropriate" individuals from roles or privileges to which they are not considered entitled. Second, they enable organizations to take coercive action against those whose behavior they consider threatening. Examples range from simply depriving minor violators of their documentation — as in revocation of driver's licenses — to arrest or imprisonment for tax fraud or other illegalities brought to light through bank records.

Personal documentation thus serves organizations by providing grounds for certainty in dealing with large numbers of otherwise anonymous individuals. It enables organizations to know what resources and actions they should apply to which individuals. Which motorists are entitled to renewed licenses, and which are wanted for serious motoring offenses by the police? Which credit card holders are entitled to the most generous credit privileges, and which are liable to arrest for fraudulent credit card use? Which passport applicants are entitled to the document as native-born citizens, and which applicants are illegal aliens seeking to travel back and forth to their country of origin? Recourse to personal documentation represents an effort to generate certainty about people in settings like these, where such certainty would otherwise be a problem for organizations.

Generating certainty about people is a problem for organizations where the interests of individuals and organizations are apt to conflict. Passports help representatives of the state distinguish between those entitled to enter their country without hindrance and others. Credit cards facilitate purchases by authorized consumers only, and control the amount of credit available to them. Whatever their other purposes, most forms of personal documentation exist at least partly to help organizations discriminate in their treatments of individuals. Most people, most of the time, may not be tempted to circumvent such discriminations — but those who are must be dealt with.

This study explores the origins, workings, and future of mass surveillance through personal documentation. How have these six documentary systems and others like them evolved? What are their strengths and weaknesses as sources of certainty for organizations dealing with the public? And what are the prospects for further growth and development in these respects?

We spent several years trying to find answers to these questions. From 1977 to 1980 we conducted interviews and observed encounters between the public and those who issue documents

at more than 34 different bureaucratic sites in the United States. These included such diverse settings as a small bank in New York State; a large bank headquarters in San Francisco; offices engaged in passport issuance in the Washington, D.C. vicinity; offices of the Department of Health, Education and Welfare in Maryland; and local, county, and state birth certification offices in New York. In many cases, these interviews and observations entailed repeated visits to the same site; a minority of the interviews were by telephone. Most interviews were with middle-level officials responsible for managing the issuance or use of personal documentation in one specific location; some were with higher-level officials more concerned with broad policy than with day-to-day operations. In addition, we analyzed a variety of published and unpublished reports on the organizations depicted in this paper.

First we chart the origins of these documentary systems and the broad patterns of their historical development. Then we look at the strengths and weaknesses of these systems as instruments of surveillance and social control. Finally, we show how the continuing perfection of technology and organization promise growing efficiency for organizational interests over the years to come.

HISTORICAL DEVELOPMENT AND SPONSORSHIP

Mass use of personal documentation is a relatively recent historical development in the United States. Of the six documents we studied, three—Social Security cards, driver's licenses, and credit cards—did not exist at the beginning of the 20th century. The other three—birth certificates, passports, and bank books—were restricted to much smaller subsets of the population than they are today. The growth in coverage and importance of these personal documents mirrors the growing role of direct relations between centralized organizations and private individuals.

Birth Certificates

Birth registration and certification have been carried out by government agencies in North America since well before the American Revolution. One of the earliest laws requiring registration of births with government agencies (as distinct from recording in parish registers) dates from Virginia in 1632 (U.S. Department of Health, Education and Welfare, 1954:3). But we estimate that the majority of births in the United States remained unrecorded with any government agency until at least the end of the 19th century. In 1903, the U.S. Congress passed a joint resolution requesting states to develop a uniform system of registering births (1954:8). Since then, federal authorities have been urging the states to increase the coverage and rigor of their registration and certification procedures. Individual states were declared part of a birth "registration area" when they had registered an estimated 90 percent of births within their boundaries (1954:8). The first states to meet this criterion—generally older, more urban ones such as Massachusetts and New York—did so in 1915; the last—Nevada, New Mexico, South Dakota, and Texas—did so between 1928 and 1933 (1954:13).

By 1950, census officials estimated that 97.9 percent of all births in the United States were being registered (U.S. Department of Health, Education and Welfare, 1954:12). Today, documentary requirements make it difficult for anyone born in the United States to do without a birth certificate; it is often essential for access to schooling, insurance, and pension coverage—as well as in applying for a variety of other personal documents. Issuing birth certificates remains a state responsibility; in 1976, there were at least 7,000 offices across the United States authorized to issue certificates or copies (U.S. Department of Justice, 1976:17). States vary enormously in the degree of centralization and rigor they apply in issuing birth certificates, according to state and federal officials we interviewed. Some states issue only through a single central office, while New York State, at the other extreme, maintains some 1,500 issuing locations. According to a

knowledgeable federal official,¹ the federal government continues to promote greater centralization and co-ordination within and among the states in birth certification – particularly in matters relating to the use of the documents for surveillance and social control. This source estimated that federal requirements, such as those for documentary substantiation of applications for Social Security cards, account directly or indirectly for about half the demand for birth certificates in the United States. By 1976, there were at least 10 million such requests per year (U.S. Department of Justice, 1976:17).

Driver's Licenses

Licensing drivers has always been a state responsibility, and as with birth certificates there has been considerable variety in practices from state to state. According to an official of the American Association of Motor Vehicle Administrators,² Massachusetts was the first state to license drivers, in 1907, and South Dakota the last, in 1957. Initially, licenses seem to have been strictly a way of generating revenue, but gradually they became a means of surveillance and control.

In 1950, there were an estimated 62 million driver's licenses in force throughout the United States. By 1978, that figure had risen to 140.8 million, and some 50.6 million new and renewed licenses were issued that year (American Association of Motor Vehicle Administrators, 1979:D-L-1). Quite beyond its role in surveillance over driving, the driver's license has become essential identification in a variety of other settings, such as check cashing and car rentals. So pervasive is the need for driver's licenses that by 1977 at least 40 states issued "non-driver's licenses" for those who did not drive, but who needed the documentation for other purposes (Tritsch and Kumbar, 1977:H-19).

Passports

Passports were first issued in North America before the Revolutionary War. It was not until 1856 that the U.S. federal government claimed exclusive rights to issue passports; until then these documents could also be issued by state and even local officials (U.S. Department of State Passport Office, 1976:31). From 1801 to 1809, the State Department issued 587 passports, while from 1898 to 1905 they issued 108,404 (1976:220). At the end of 1978 there were some 13.9 million valid, domestically issued U.S. passports (as distinct from those issued by U.S. officials abroad) and some 3.2 million new passports were issued that year.³

The growth in passport use is attributable both to the rise in international travel and to the development of the modern state. During the 19th century, few countries required the use of passports except in wartime. The United States did not require U.S. nationals to use passports for travel in peacetime until 1952, and it is estimated that most U.S. travellers did not carry passports in peacetime until the late 1940s (1976:4).

Social Security Cards

Social Security was founded through legislation passed in 1935 (Booth, 1973:7), and 45 million accounts were opened by the end of the first year the system was in operation (Westin and Baker, 1972:33). Because of the advantages associated with participation in Social Security, the number of accounts rose quickly to approximate the number of employed persons. By mid-1983, accord-

1. Loren Chancellor, Registration Methods Branch Chief, Department of Health, Education and Welfare, Rockville, Maryland, May 11, 1977: personal interview.

2. Arthur Tritsch, Director, Driver Services, American Association of Motor Vehicle Administrators, Washington, D.C., May 23, 1983: telephone interview.

3. Norbert J. Krieg, Deputy Assistant Secretary for Passport Services, November 14, 1979: personal communication.

ing to a Social Security official, there were 205 million active accounts, each with a Social Security number and card corresponding to it. Some 5.5 million new accounts are being added each year.⁴ Because nearly every economically active adult in the United States has a Social Security number, the number is ideal for other surveillance and management purposes. Since 1961, the Internal Revenue Service (IRS) has adopted the use of Social Security numbers for ordering income tax records and for identifying taxpayers.⁵

Credit Cards

The earliest credit cards in the United States, available for relatively narrow ranges of products and services, appear to have been issued in the early decades of the 20th century (Rule, 1974:225). Some general-purpose cards catering to affluent users (e.g., Diner's Club, Carte Blanche) were issued in the decade or so after the Second World War. But it was not until banks began issuing credit cards to middle and even lower-middle income groups that the majority of the adult population gained access to this form of documentary relationship. Today VISA and MasterCard account for virtually all of the bank-issued credit cards in use in the United States. In 1978, there were some 52 million MasterCard and 54 million VISA cards in use, and these two systems issued some eight and 10 million new cards respectively that year (American Bankers Association, 1979).

In 1979, responsibility for issuing and managing VISA and MasterCard accounts was dispersed among 10,600 and 11,000 banks respectively throughout the United States (American Bankers Association, 1979). These thousands of companies observe a variety of policies, but all maintain careful surveillance and control over issuance and use of their cards. All exchange information and other services with other surveillance and control organizations, as we discuss below. Partly because of the sophistication of surveillance and control achieved by the managers of VISA and MasterCard, the cards have become required for use in other transactions such as cashing checks and renting cars.

Bank Books

According to officials of the American Bankers Association, only a small minority of U.S. families had bank accounts at the beginning of the 20th century. By 1977, however, 77 percent of U.S. families had checking accounts, and 81 percent had savings accounts — including accounts both in banks and savings and loan institutions (Curtin and Neubig, 1979:22).

THE PURSUIT OF CERTAINTY: SELF-IDENTIFICATION

Organizations use systems of personal documentation to cope with people who attempt to circumvent organizational purposes by concealing or distorting information about themselves. The importance of this task warrants the considerable expense and effort of building and maintaining the bureaucratic systems which stand behind these personal documents. But how well do these bureaucratic activities serve the surveillance goals for which they are intended? One of the first things to strike us as we began this study was the wealth of apparent opportunities for circumventing the surveillance purposes of the six systems we looked at: in fact, it is easy to obtain these six personal documents under false pretenses. We make this observation not to appeal for tighter controls, but to note a sociological puzzle: personal documents which are widely regarded as authoritative, and which figure in important bureaucratic surveillance processes, often do not seem to warrant the credence placed in them.

4. Nicky Bonacci, Press Office, Social Security Administration, Woodlawn, Maryland, July 8, 1983: telephone interview.

5. Income tax was first collected in peacetime in 1913. By the eve of the Second World War, according to an IRS official, only about 8 million U.S. citizens paid federal income tax, a small minority of the adult

These weaknesses seem particularly marked where organizations must rely on applicants' own accounts, and upon documents presented by applicants, in deciding whether to issue documentary identification. For example, birth certificates are widely perceived as a basic and trustworthy form of identification and are used to generate other personal documents. Yet officials in organizations relying on birth certificates for surveillance acknowledge that these documents can be easily obtained fraudulently. People who wish to conceal their true identities may check obituaries or other death records of persons about their own age, then request a birth certificate in the name of the deceased person (U.S. Department of Justice, 1976:19). The widely varying rigor among offices issuing birth certificates makes this practice quite easy. A few states seek to restrict dissemination of certificates by requiring a signed statement establishing a "legitimate need" for the document. But others officially grant anyone the right to obtain a certified copy of any birth certificate which can be identified (1976:18). Since certificates and official copies of certificates issued in the United States provide no way of identifying the person presenting the document with the person whose birth is recorded there, consumers of birth certificates normally have only the individual's own account to establish this link.

Nevertheless, self-identification *via* the birth certificate plays a key role in generating other personal documents. Issuance of driver's licenses, for example, depends overwhelmingly on self-identification by the applicant. Indeed, as recently as 1977 several states required no personal document to substantiate information on driver's license applications. Where supporting documentation is required, the birth certificate is by far the document most often used (Tritsch and Kumbar, 1977:D-1). Other documents acceptable in applying for a driver's license, such as baptismal certificates or the Social Security card, are also readily available under false pretenses. For female applicants, the family name given on the birth certificate or other documents dating from before marriage need not agree with the name in which the license is sought. Our observations of driver's license issuance in New York State convinced us that the face-to-face transactions between applicants and staff were much too superficial to enable the latter to verify the authenticity of substantiating documents. We doubt that greater scrutiny is the rule elsewhere (U.S. Department of Justice, 1976:F-15).

Social Security cards are also issued almost entirely on the basis of self-identification. Prior to 1974, applicants were not required to produce supporting documentation (U.S. Department of Justice, 1976:24). Among documents currently used for this purpose are birth certificates, library cards, and voter registration cards, all readily obtainable under false pretenses (U.S. Department of Health and Human Services, 1982). One official whose work involved issuing Social Security cards reported that she was instructed to issue cards on presentation of the officially required documentation, even if applicants' accounts of their background and circumstances were blatantly implausible.⁶

Passports are issued with only slightly more rigor than Social Security cards. Passport applications must be submitted in person, and passport officials are supposed to question applicants about details put forward there. This first stage of the application process is aimed at establishing the applicant's identity; one of the documents most widely used for this purpose is the driver's license (U.S. Department of Justice, 1976:21). Passport officials are supposed to question applicants about statements on their applications and about the accompanying identification; the exchanges we observed appeared more perfunctory than probing, lasting about 10 to 15 minutes. The application is then forwarded to a central location, where officials scrutinize further supporting documents to determine the applicant's citizenship. The document most often used for this purpose, according to passport officials, is the birth certificate.

Reliance on self-identification in the issuing of personal documentation leads to a kind of

⁶ Social Security official, San Francisco, August 10, 1979.

chain-reaction process, in which acquisition of a birth certificate affords access to a succession of further documents. Each item of documentary identification strengthens the case for access to further items. Not only the birth certificate, but also other documents even more easily available under false pretenses—such as voter's registration cards—serve as "breeder documents," each etching the holder's documentary identity more deeply in a document-oriented world.

A SUPERIOR SOURCE OF CERTAINTY: DIRECT CHECKING

The dilemma facing organizations is clear. Surveillance systems are developed to enable organizations to distinguish between those worthy of friendly treatment and others. Yet self-identification leaves the responsibility of transmitting vital data in the hands of the very people who may be tempted to seek a "better deal" of some kind by circumventing the purpose of the system.

But superior techniques of surveillance are increasingly available. Organizations can use direct channels to move personal data from points of origin to where they are needed for decision-making without requiring the interested individuals to act as intermediaries. Reliance on such direct checking both helps reduce the costs of dealing with individual documents on a one-by-one basis and, more importantly, obviates the weaknesses inherent in direct checking.

Direct checking is essential in screening VISA and MasterCard applications. Supporting documents are rarely required here, and crucial information provided on application forms is nearly always checked against data from independent, outside sources—usually credit bureaus. These are profit-making firms which specialize in compiling and selling data on consumers' credit-worthiness. They either confirm or supply information on applicants' current indebtedness, past payment of credit accounts, and history of litigation, liens, bankruptcies, and the like. Where data from credit bureaus are lacking, credit card firms may rely on other forms of direct checking, such as telephone contacts with applicants' employers or banks to determine their salary and financial status. Exchange of such information among these organizations is a routine part of their clerical practice.

Direct checking also plays a key role in surveillance over the ongoing use of credit cards. VISA and MasterCard maintain elaborate systems to monitor use of their cards, both by intended users and by criminals. One way they do this is by continually analyzing records of purchases made with cards, to detect overspending and fraud. Another is by requiring that certain large charges be first cleared by telephone with the bank which issues the card (Rule, 1974:240). The latter form of direct checking sometimes leads to the arrest of fraudulent users before they leave the store. BankAmericard (predecessor of VISA) reported making 450 such arrests in California alone in 1970 (Rule, 1974:246).

Direct checking is also used in processing driver's license applications. Many states rely on their own data files compiled by state police and courts. Other states check license applications against the National Driver Register, a computerized central listing of persons whose licenses have been revoked or suspended throughout the United States. The latter practice was used in 26 states in 1977 (Tritsch and Kumbar, 1977:B-1). During 1978, the National Driver Register reported 180,000 "hits," or probable identifications of ineligible persons seeking new licenses; most of these no doubt resulted in denials of new licenses. In addition to the National Driver Register, the National Law Enforcement Telecommunications Network (NLETS) acts as a central switchboard for direct checking on drivers by law enforcement agencies throughout the United States; for example, it can determine whether an out-of-state driver's license is valid where issued (U.S. Congress, Office of Technology Assessment, 1982:40). In March 1983 alone, according to an NLETS official,⁷ this system handled about half a million such interstate inquiries.

7. Tim Sweeney, National Law Enforcement Telecommunications Network, Phoenix, Arizona, May 11, 1983.

Direct checking is an option in issuing other forms of documentary identification as well. Requests for *duplicate* Social Security cards are checked with data on the card-holder held in central files before the duplicate is issued. Similarly, passport authorities can sometimes directly check documents submitted with passport applications. But such checks are unlikely unless the documents appear inauthentic; applicants bent on fraud may simply submit authentic documents referring to someone else.

Direct checking in surveillance over the use of passports, however, is well developed. The Treasury Department has developed a comprehensive computerized data base against which it checks the names of many incoming travellers as they cross the U.S. border. The goal is to extend these checks, which apply both to U.S. nationals and foreigners, to all such travellers, though present rates of coverage are uneven among the many border points. The data base includes the names of persons whose movements are of interest to a wide variety of local, state, and federal officials. Part of the data base consists of the FBI's computerized listing of wanted and missing persons from throughout the United States. During 1978, some 49.7 million persons and vehicles were checked against this listing as they entered the United States; 21,760 "hits" were made in this way, and 2,070 persons were arrested as a result.⁸ In some instances government agencies are unable or unwilling to authorize arrest, but nevertheless have the system retain a record of the person's movements.

Finally, direct checking is sometimes involved in issuing savings passbooks and check books. Banks try to confirm the identities of those seeking to open accounts when they doubt the applicant's background. If they suspect an account is being sought for fraudulent purposes such as writing bad checks, bank officials may contact the applicant's employer or personal and business references. Banks appear responsive, in these matters, both to their own interests in avoiding fraud and those of local businesses and law-enforcement agencies.

Symbiosis in surveillance: the elaboration of direct checking

The six personal documentation systems also act as *sources* of personal data for direct checking by other organizations. These flows of data across organizational lines are taking on increasing importance in the national organization of mass surveillance in the United States. The fact that more and more routine bureaucratic paper work is being done electronically means that organizations have more personal data to offer one another. Such symbiotic relations among organizations warrant close attention.

Ironically, birth certification is perhaps the least developed of these six systems in this respect. Certificates and certified copies are readily available, but the means of disseminating them are relatively primitive. Organizations seeking birth certificate information must normally depend on the person whose birth is certified, because of the difficulty of identifying the source of the certificate and obtaining it independently. New social structures and technologies which would transmit birth certificate data directly from its source to organizational consumers — as readily, say, as credit reports — would surely be a boon to the organizations concerned.

By contrast, data from driver's license files are provided freely to outside interests. Police forces and other law enforcement agencies share data via the NLETS. The next most frequent users of driver's license data are undoubtedly insurance companies, who seek the data for screening and processing insurance applications. In 1976, all but two states made at least some data from a driver's record available to insurance companies. Nineteen states routinely granted access to the entire record, and many states realized significant revenues ranging from eight cents to four dollars per inquiry (Tritsch and Kumbar, 1977:H-11). The volume of data so provided can be great. The state of Illinois in 1982 answered some 2.5 million requests for data from driver's license files.

8. Jay Corcoran, Director, Information Services Staff, Department of the Treasury, U.S. Customs Service, March 3, 1981: personal communication.

About 179,000 of these were from law-enforcement officials; the overwhelming balance no doubt came from insurance companies (State of Illinois, 1983).

Information from Social Security files, including both income data and the account-holder's whereabouts, is intensely attractive to many outside interests. When the Social Security system was founded in 1935, elaborate assurances were offered that data would remain confidential (Rubinstein, 1975). But confidentiality has been eroded over the years, especially since the 1970s. Social Security files are now open to state welfare departments and food stamp programs (to control access to benefits), the FBI and the Secret Service, the Immigration and Naturalization Service (to control employment of undocumented aliens), and others (U.S. Department of Health, Education and Welfare, 1977:52239). One of the more controversial users of Social Security information is the Parent Locator Service. This agency, established by Congress in 1975, uses such data for action against parents who desert spouses with dependent children (U.S. Privacy Protection Study Commission, 1977b:16). In creating the service, Congress also granted it access to personal data held by other federal agencies, including the Internal Revenue Service.

Data generated by credit card companies are provided routinely to a variety of organizations. Probably the biggest data consumers are credit bureaus, who normally demand an exchange of data: organizations which purchase the credit bureaus' reports must then provide data from their own files. Such data are increasingly provided in large quantity by direct computer links. In addition, many credit card issuers provide the addresses of card holders to merchants who have accepted the card as identification for a check which subsequently bounced. This is apparently why credit cards are so often preferred as identification in check cashing: the merchant may have no other way of contacting the writer of the check. Credit card issuers help merchants in this way because of their shared desire to control bad checks written by card-holders. Credit card firms, like most other large-scale creditors, also provide information from their files to law-enforcement agencies, including the Internal Revenue Service, the FBI, and other local, state, and federal bodies. Data of interest here include the amounts of the card-holder's indebtedness and the nature of expenditures, as well as the individual's whereabouts at particular times (U.S. Privacy Protection Study Commission, 1977a:53).

Finally, data generated through use of checking and savings accounts are regularly provided to credit bureaus, prospective creditors, and a variety of law enforcement agencies. The effects of such provision, in terms of social control, range from extension or withdrawal of credit to prosecution for tax evasion and other felonies. A few banks and savings institutions resist such disclosure, but these seem to be a distinct minority (Linowes, 1979:11). Demands from law-enforcement agencies for data are often backed by subpoena, leaving court action the only available avenue for resistance.

Besides responding to inquiries from such outside bodies, savings institutions are required to report yearly to the federal government all interest paid to depositors. Such institutions also must report foreign currency transactions in excess of \$10,000 (U.S. Privacy Protection Study Commission, 1977a:104). And, in compliance with still other federal regulations, virtually *all* personal checks paid by United States banks are microfilmed; the records are retained for five years to be available for scrutiny by federal officials (U.S. Privacy Protection Study Commission, 1977a:105).

THE FUTURE OF MASS SURVEILLANCE

The dramatic proliferation of personal documentation since the beginning of the 20th century means much more than growing possession of certificates, cards, and computer records. It reflects the growth of an important new category of *relationships* between ordinary people and large, centralized organizations. These new relationships entail increasing demands on personal privacy, as organizations consume more and more personal data and use these data to shape their treatment of persons with whom they deal. As we have shown, these demands are growing apace with the

further refinement of technological and organizational resources. Where, we must ask, are these trends leading? What sort of social world is emerging from the changes detailed here?

To answer such questions, one must consider the limitations of organizational mass surveillance as much as its strengths. These limitations are by no means trivial. Organizations cannot achieve mass surveillance goals without data, and such data are by no means available simply for the asking. Indeed, we have shown how even the most seemingly powerful organizations often must accept significant limitations on their ability to master important data on the people with whom they deal.

A key example is the widespread reliance on self-identification, including personal documentation presented by those being identified. It is widely acknowledged by officials of surveillance organizations that such practices as permitting people to provide their own birth certificates lead to significant evasion of social control. Yet the organization of information flow in the United States does not yet offer an alternative to these practices at acceptable cost.

Similarly, some organizations do not even exploit relevant data already contained in files accessible to them. This is true of some state driver's licensing systems, which issue licenses on the strength of data provided by the applicants, without checking their own records of the applicants' driving histories (Tritsch and Kumbar, 1977:2-1). Here, we conclude, organizations are responding both to the costs of clerical time in searching for potentially relevant data, and to costs in terms of public complaints over delays in issuing documents. A number of officials reported that the latter were an especially important consideration for their organizations. This appears particularly true for the four government documents: birth certificates, passports, driver's licenses, and Social Security cards. The public are apt to insist on quick access to these as a matter of right (U.S. Department of Justice, 1976:F-15).

Still, the effect of such weaknesses in surveillance may be a good deal less than it would appear. Organizations do not advertise the laxity of their surveillance procedures. They are much more likely to require applicants to read and sign statements such as the following, from the application for Social Security cards:

WARNING: Deliberately furnishing (or causing to be furnished) false information on this application is a crime punishable by fine or imprisonment, or both (U.S. Department of Health and Human Services, Social Security Administration, 1982).

In fact, fraudulent applications for Social Security cards are rarely prosecuted unless they are compounded with other, more serious infractions. There were 117 prosecutions and 62 convictions in the years 1980 to 1982 inclusive, according to a Social Security official.⁹

The effectiveness of mass surveillance and social control depends most directly on the public's *perceptions* of what systems can and cannot know about them. Most U.S. citizens are apparently aware that large organizations are capable of sophisticated data linkages. They realize that income not listed on tax returns is likely to be reported directly to the Internal Revenue Service by the paying organization, or that creditors have ways of finding out about debts not acknowledged on credit applications. But relatively few people, we suspect, can distinguish between the risk that a credit applicant's recent bankruptcy will be reported to a prospective creditor and the risk that the Passport Office will spot an application for a passport in the name of someone who already has one. The first risk is relatively great, since credit bureaus systematically collect and report such data, while the second is relatively low, since the Passport Office ordinarily does not check new applications against records of outstanding passports.

The overall picture that emerges from these observations is one of dialectical tension between

9. Robert Sedlak, Inspector General's Office, Department of Health and Human Services, Baltimore, May 13, 1983; telephone interview.

the efforts of organizations to maximize the scope and effectiveness of mass surveillance, and the efforts of certain subsets of the public to evade organizational intent in these respects. Organizational reliance on bluff and intimidation is part of one side of this dialectic; yet such feints would mean little without the other weighty organizational efforts considered here — particularly the development and exploitation of new sources of data. Countervailing against such forces are individuals' efforts to escape the effects of bad credit records, poor driving histories, ineligibility to enter the United States, and the like.

We do not portray this opposition in simplistic terms, as nothing other than efforts by oppressive institutional interests to manipulate innocent individuals. In fact, there is considerable grassroots support and even demand for increased mass surveillance — for example, to keep undocumented aliens out of the labor force, to keep dangerous drivers off the roads, or to keep poor credit risks from spoiling the credit markets enjoyed by others. But whatever the mixture of elite initiatives and popular demand fueling the growth of mass surveillance, there can be no doubt that organizational powers in this respect are in the ascent, and opportunities for individual evasion of mass surveillance increasingly restricted.

The key consideration mediating the interests of mass surveillance and those of evasion are the significant *costs* of the former. While the per-case costs of operating large data systems is ordinarily small, the starting-up costs of creating such systems is great. Thus, even relatively powerful and well-financed organizations such as those considered in this paper cannot extend their sway as rapidly as they might. Paying the armies of clerical staff who must assemble and process personal data is one significant source of these costs; procuring and operating computing systems and other data-management technologies are another. Yet the conspicuous trend in mass surveillance is toward a cumulative decline in such costs.

Consider the growing reliance of organizations on direct checking, as distinct from self-identification. At the beginning of the 20th century there were few organizations which could be counted on to generate authoritative personal information on a mass basis. Even birth certification probably covered no more than half of those being born. And without sources of "breeder documents," the bases for generating further documents were weak.

As sources of authoritative personal data available for direct checking grow, however, the costs of mass surveillance drop. Indeed, viewing the broad sweep of historical change, we conclude that *mass surveillance through personal documentation feeds on itself*. The more important events in life entail production or consumption of personal documentation, the more feasible it is to institute effective surveillance through direct checking based on such data. Imaginative administrators of surveillance organizations are constantly seeking new uses for personal data in these ways.

This, then, is the special appeal of direct checking, from the standpoint of surveillance interests. When accomplished through computer links, it is relatively inexpensive on a per-case basis, extremely quick, and unobtrusive from the standpoint of the individuals involved. These same qualities both excite the enthusiasm of bureaucratic planners and politicians and spur the anxiety of privacy advocates and civil libertarians. In the last few years, the former have been putting their concerns aggressively into practice, while the latter have mostly been on the defensive. One of the best publicized instances of new forms of mass surveillance through low-cost direct checking have been the programs of "computer matching" sponsored by federal agencies. Here computerized lists of, say, welfare recipients are checked against other computerized data such as payrolls in order to detect fraud. Originally sponsored by Joseph Califano during his tenure as President Jimmy Carter's Secretary of Health, Education and Welfare, these efforts have been pursued with increased vigor under the administration of President Ronald Reagan. Proponents of these techniques have lauded them as essential to government efficiency and cost-cutting; opponents have characterized them as violations of due process, privacy, and civil liber-

ties. Both positions were voiced in the 1982 hearings of the Subcommittee on Oversight of Government Management of the Senate Government Affairs Committee (U.S. Congress: Senate, 1983).

The perfection of direct checking within and among organizations is the wave of the future in mass surveillance. By substituting direct checking for self-identification, organizations can transcend the limitations which have beset mass surveillance in the past, and which continue to limit the effectiveness of a number of the processes described above. Instead of relying on individuals to provide information and documents themselves, organizations will increasingly seek personal data directly from other organizations. Such exchanges will increasingly take the form of computers talking to computers. And as data management in all kinds of organizations becomes computerized, the machines will have more and more to talk about. Such exchanges will transcend limitations on mass surveillance and control in the interests of enhanced efficiency.

But inefficiency may protect important values. Whatever one thinks of the goals of specific surveillance procedures, few really want to see the ability of organizations to keep track of people grow without limit. At best, such developments would foster a more intrusive, less private world. At worst, they would lower institutional defenses against threats of totalitarianism. Thus, we favor limitations on direct checking in many settings, especially where personal data provided for one purpose are re-used for another purpose unfriendly to the individual (Rule *et al.*, 1980:153). We hope this study helps to show what is at stake in these developments, and what price is paid for making personal documentation and mass surveillance more efficient.

REFERENCES

- American Association of Motor Vehicle Administrators
 1979 Driver's License. 1978. Statistical Report. Washington, D.C.: American Association of Motor Vehicle Administrators.
- American Bankers Association
 1979 ABA Bank Card Letter, March 1979. Periodical. New York: American Bankers Association.
- Booth, Philip
 1973 Social Security in America. Ann Arbor, Michigan: Institute of Industrial and Labor Relations, University of Michigan and Wayne State University.
- Curtin, Richard T., and Thomas S. Neubig
 1979 Survey of Consumer Finances 1977-78. Ann Arbor, Michigan: Survey Research Center, University of Michigan.
- Linowes, David
 1979 "Privacy in banking." Mimeograph. University of Illinois, 308 Lincoln Hall, Urbana, Illinois.
- Rubinstein, Walter D.
 1975 Confidentiality Under the Social Security Act. Pamphlet. Woodlawn, Maryland: Social Security Administration.
- Rule, James B.
 1974 Private Lives and Public Surveillance. New York: Schocken.
- Rule, James, Douglas McAdam, Linda Stearns, and David Uglow
 1980 The Politics of Privacy. New York: Elsevier.
- Shils, Edward
 1975 Center and Periphery: Essays in Macrosociology. Chicago: University of Chicago Press.
- State of Illinois
 1983 Report of State Advisory Committee on Distribution of Government Information. Springfield: Office of the Secretary of State.
- Iritsch, Arthur, and Albert Kumbur
 1977 Comparative Data Analysis of State Motor Vehicle Administration. Washington, D.C.: National Highway Traffic Safety Administration.
- U.S. Congress, Office of Technology Assessment
 1982 An Assessment of Alternatives for a National Computerized Criminal History System. Washington, D.C.: Office of Technology Assessment.
- U.S. Congress: Senate
 1983 Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs. Committee on Governmental Affairs, Subcommittee on Oversight of Government Management, 97th Congress, 2nd Session. Washington, D.C.: U.S. Government Printing Office.

- U.S. Department of Health and Human Services, Social Security Administration
 1982 Application for a Social Security Number. Flyer. Washington, D.C.: U.S. Government Printing Office.
- U.S. Department of Health, Education and Welfare
 1954 Vital Statistics of the United States, 1950, Volume I. Washington, D.C.: U.S. Government Printing Office.
 1977 Privacy Act Issuances. Annual Publication, Federal Register. Washington, D.C.: U.S. Government Printing Office.
- U.S. Department of Justice
 1976 The Criminal Use of False Identification. Washington, D.C.: U.S. Government Printing Office.
- U.S. Department of State, Passport Office
 1976 The United States Passport: Past, Present, Future. Washington, D.C.: U.S. Government Printing Office.
- U.S. Privacy Protection Study Commission
 1977a Personal Privacy in an Information Society. Washington, D.C.: U.S. Government Printing Office.
 1977b Citizen as Taxpayer. Washington, D.C.: U.S. Government Printing Office.
- Westin, Alan
 1967 Privacy and Freedom. New York: Atheneum.
- Westin, Alan, and Michael Baker
 1972 Data Banks in a Free Society. New York: Quadrangle Books.
- Wheeler, Stanton (ed.)
 1969 On Record. Files and Dossiers in American Life. New York: Russell Sage Foundation.

[From the New York Times, Dec. 8, 1983]

PRIVACY THREATS WORRY AMERICANS

MANY IN SURVEY BELIEVE DATA ON TAXES AND TELEPHONES ARE NOT KEPT SECRET

(By Adam Clymer)

WASHINGTON, Dec. 7.—Americans are increasingly concerned about threats to privacy, and about a third of the public believes the Internal Revenue Service, the Federal Bureau of Investigation and telephone companies “probably share” information on individuals with others, according to a poll conducted by Louis Harris and Associates.

Results of the Sept. 1-11 survey of 1,256 people, paid for by Southern New England Telephone Company, were released today as the Smithsonian Institution opened a four-day symposium on “The Road after 1984: High Technology and Human Freedom.”

Participants will examine various aspects of society in light of George Orwell’s novel “1984,” which foresaw an almost all-powerful government.

The telephone poll found the percentage of Americans who said they were “very concerned” about threats to personal privacy increased from 31 percent in 1978 to 48 percent in 1983. It found four Americans in five believed it would be easy for someone to assemble a master file on their lives that would violate their privacy.

SHARING OF INFORMATION

The poll found that 84 percent of the public thought it would be a serious violation of privacy if the revenue service did not keep tax returns confidential, and 82 percent thought it would be serious if the F.B.I. did not keep its data secret.

When asked what they thought actually happened to such data, 36 percent of the respondents said they thought the revenue service shared information and 38 percent said they believed the F.B.I. did. Thirty-three percent said they thought phone companies shared data, although 25 percent said phone companies did not have any information that mattered.

Those agencies were trusted more than several other institutions presented. Fifty percent of the public thought public opinion research concerns shared data, and 51 percent said the Census Bureau, banks and government welfare agencies did so. Fifty-seven percent said they believed insurance companies shared their information, 65 percent said this of loan companies and 75 percent said credit bureaus shared information with others.

Along with the telephone sample of the 1,256 people, the pollsters also interviewed 100 leaders in each of four categories; members of Congress and their aides, corporate executives, science editors and school superintendents. In general, those groups were less fearful of major invasions of privacy than the public was.

LEADERS’ OPINIONS DIFFERED

For example, 86 percent in the sample of the public thought it was possible that “a government in Washington will use confidential information to intimidate individuals or groups it feels are its enemies,” and 70 percent said that was “likely.”

All four leadership groups also said such a development was possible, by about the same percentages as the public. But just 24 percent of the congressional group, 37 percent of the executives, 56 percent of the editors and 39 percent of the school superintendents said it was “likely.”

Mr. Harris, chairman and founder of the polling concern, commenting on the findings at a news conference, said he believed “the leadership is far less alerted to the dangers than the people are.”

“Those at the throttle of our political leadership just haven’t given it much thought,” he said.

[From the New York Times, Dec. 25, 1983]

IRS STARTS HUNT FOR TAX EVADERS, USING MAIL-ORDER CONCERNS’ LIST

(By David Burnham)

WASHINGTON, Dec. 24—The Internal Revenue Service has obtained a computerized mail-order list of the estimated incomes of two million American households

and has begun to test whether it can help track down people who fail to pay their taxes.

The service is conducting the test despite the refusal of the three major companies that develop such information to provide the Government with a list and over the objections of their trade organization, the Direct Marketing Association.

Alexander Hoffman, who is the chairman of the board of the association and a group vice president at Doubleday & Company, said the sale of the list to the I.R.S. violated a provision in the group's code of ethics that lists should be rented only for marketing and could "upset an important segment of the economy."

The revenue service said a brokerage firm that provides marketing lists, the Dunhill Company of Washington, D.C., had put together the names the agency sought. The association said the company was not one of its members. Officials at the company did not return several telephone calls, but the revenue service spokesman said the names had been put together from several small concerns.

BROOKLYN INCLUDED IN TEST

In the test, a commercially prepared list of two million households in Brooklyn, Wisconsin, Indiana, and Nevada will be matched against an I.R.S. list of people living in those areas who filed income tax returns for the tax year 1982.

All those whose names appear on the first list, but not the second, will be notified that they are subject to a revenue service inquiry about their tax liability. The notices will start going out next spring. An executive of one of the companies objected to the test on the ground that many people who have not done anything wrong get the notices.

If the test identifies individuals who file no taxes at all, the service will then try to determine whether the same technique can be used to track those who underpay their taxes. According to an I.R.S. plan the decision whether to use the technique nationwide will not be made until 1985 or later.

A spokesman for the revenue agency said the commercial list is obtained for its test match, after a five-month search, contained the names and addresses of two million households, their estimated incomes, the birthday of the head of each household and the number of people living in each.

In the last few years, the tax agency has become concerned about a slow increase in the number of Americans who fail to pay their taxes. Because of this concern, the agency has sought to develop new techniques for identifying tax evaders.

A recent I.R.S. report on income tax compliance, for example, estimated that revenue losses caused by people compile national mailing lists, the Donnelly Marketing Service of Stanford, Conn. the R.L. Polk Company of Detroit and Metromail of Lincoln, Neb., decided this fall not to sell their information to the tax agency. In separate interviews officials of the three companies called the project "absolutely ridiculous" and "inappropriate" and indicated it would hurt their business.

The revenue service said a brokerage firm provides marketing lists, the Dunhill Company of Washington, D.C., had put together the names the agency sought. Officials at the company did not return several telephone calls, but the revenue service spokesman said the names has been put together from several small concerns.

Mr. Hoffman, the current head of the 2,600-member Direct Marketing Association, said in a telephone interview that he understood that the tax agency had a legitimate concern and that he and his organization hesitated about making "a big public pronouncement" that might affect the Government's ability to handle a real problem.

"But there are some questions we feel the I.R.S. should consider," he said. "What effect will the I.R.S. use of mailing lists have on the public's perception about this kind of communication? What I am worried about is that if the I.R.S. is able to undertake this effort on a national basis, it may make the public afraid to have their name on any mailing list, afraid to buy anything buy mail, afraid to fill out coupons. By conservative estimates, direct marketing now accounts for sales totaling \$140 billion a year."

DIFFERENCE IS NOTED

Mr. Hoffman said there was a very real difference between the commercial use of a mailing list and the use being explored by the tax agency. "Strangely enough, a mailing list is essentially anonymous," he said. "A company rents a computer tape, prepares one set of labels and makes a mailing. That's it. If you want to have your name removed from a particular list or all lists, our organization operates the Mail Preference Service at 6 East 43d Street in New York where this can be accomplished.

"But if the I.R.S. starts with a commercial mailing list, then adds Census data, then cross references it with other data," Mr. Hoffman continued, "then they are taking something that is essentially anonymous in the commercial world and turning it into individually identifiable information, using it in a way the individual never imagined."

Noting that the company that was said to have sold the list to the tax agency was not a member of the association, Mr. Hoffman said the sale violated one of the provisions of the group's ethical guidelines, that lists should be rented only "to persons who are going to use them for marketing purposes."

The guideline of the trade organization parallels one of the important principles set out in the Federal Privacy Act. The principle is that information collected by an agency for one purpose should not be used for another purpose without informing the individual who provided the information.

CONCERN AMONG POLLSTERS

The Council of American Survey Research Organizations, representing more than 105 public opinion firms, is also concerned about the tax agency's project.

John Rupp, a lawyer for the council in Washington, said, "We think it would be unethical for the I.R.S. or any other entity to use information obtained from individuals under a promise of confidentiality or to use information in a way that is inconsistent with the purpose for which it initially was collected."

Mr. Rupp added that the council would support the Federal project as long as it was completely based on information in public files. But he added; "In a democracy as complex and varied as ours, that polling plays a pivotal role. We worry that survey or marketing research may not long survive if the trust of the American people is undermined."

Because the original sources of the computerized names provided to the revenue service are unknown, it is not possible to determine how the data were collated.

The method used by the Donnelly Marketing Service, however, involves placing in computer the names and addresses taken from every telephone book as it is published. The computer is then instructed to assign each household to the correct census tract. From the information published by the Census Bureau, conclusions can be made about each household, including median income, average family size and probable race.

In those states where the information is available on a computerized list, Donnelly then matches data from the Department of Motor Vehicles on the model and year of automobiles owned by the individuals at each address. If the auto is an expensive one, the estimated income is adjusted upward; if it is a cheap model, the income is reduced.

Reginald C. Troncone, the executive vice president of Metromail, recently expressed his concern about the I.R.S. project in a letter to Representative Doug Barnard Jr., the Georgia Democrat who is chairman of the House Government Operations Subcommittee on Commerce, Consumer and Monetary Affairs.

"Our company is caught in the middle," he said. "There isn't any way the I.R.S. can conduct the proposed program and come up with a list of only those individuals who have not filed tax returns. There will be literally millions of legitimate filers who will be contacted by the I.R.S. to provide proof of filing a return."

Computer Communications Vulnerable As Privacy Laws Lag Behind Technology

No federal law clearly makes it a crime to intercept computer transmissions or to break into a computer system to look around or destroy information.

BY RONALD BROWNSTEIN

When Citicorp vice president Richard W. Coughenour wants to send a memorandum to one of the bank's employees, he turns to a compact device on the corner of his desk that looks like a cross between a computer and a telephone. The machine, called a Displayphone, has the typewriter-like keyboard and video display screen of a computer and the touch sensitive key pad of a fancy telephone.

Coughenour hits a touch pad labeled EZmail and the machine dials the number to connect him with Citicorp's internal electronic mail system, the electronic tones softly tolling as the Displayphone runs through the digits. When the number is dialed, Coughenour hits a touch pad labeled connect and the screen lights up with commands. First it asks him to enter his mailbox number. Then it asks for his password.

To send a memo, Coughenour hits a touch pad labeled compose and pulls out the small keyboard from under the pad. He types out the message and hits the touch pad labeled send.

From his office at the tip of Wall Street, the message skitters across the bank's private fiber optic cables to Citicorp's Park Ave. office. From there, if it is traveling to a Citicorp office outside New York City, the message rides a microwave relay to a private earth station in New Jersey where it is transmitted 22,300 miles up to a satellite on which Citicorp owns space. From the satellite, the message returns to another Citicorp earth station and then along public or leased phone lines to the recipient's computer. All in a matter of seconds.

Although the message is easy to send, it is also easy to steal. With a large enough antenna, it is not difficult to intercept microwave transmissions.

Is anybody listening in? "I don't doubt it," said Coughenour, a former Air Force intelligence officer who runs Citicorp's mail services. "The Russians have a big mission at the United Nations and all that equipment on the roof; that's not all there to get Home Box Office. I don't wonder if [some of our competitors] are pointing some stuff at us too."

The information may be vulnerable in a legal sense as well. While the laws governing wiretapping clearly protect spoken communications—essentially, ordinary telephone calls—many experts are concerned that no law makes it a crime to eavesdrop on communications between two computers, even though the information that passes between them is often highly sensitive.

The fuzziness of the laws protecting computer-to-computer communications is only one area where new computer or communications technologies, or merely new and aggressive applications of existing technologies, have exposed gray spots in the nation's laws governing privacy. "Our laws have not kept pace with the technology," said attorney Ronald L. Plesser, former general counsel of the Privacy Protection Study Commission, which studied the nation's privacy laws for Congress in the mid-1970s. "The technology has been expanding so quickly that the laws written for one level of technology quickly become obsolete."

Generally, the privacy implications of these technological changes have not received much political, legal or social attention. "We're not even giving it serious, practical consideration," said University of Illinois political economy professor David F. Linowes, who chaired the privacy commission.

But with the arrival of George Orwell's nightmare year of 1984, these blind spots in the law and the general issue of privacy are beginning to receive increased ser-

tiny. *New York Times* reporter David Burnham has reignited a debate on the potential threat to privacy posed by the use of computers with a controversial new book, *The Rise of the Computer State*. Robert W. Kastenmeier, D-Wis., who chairs the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, has begun a wide-ranging series of hearings on the state of civil liberties, including the impact of new technology on privacy. Several other committees are examining the laws safeguarding computer information. Universities and other organizations across the country, such as the Smithsonian Institution, are holding conferences on Orwell, technology and 1984. And the American Civil Liberties Union is planning a major conference on privacy.

Many of these forums will be used to criticize the Reagan Administration's policies on release of government information, classification of government documents and law enforcement. But most of these groups are also examining a different issue: where has new technology outflanked the privacy laws?

ELECTRONIC MAIL

A new technology almost entirely unaddressed by existing law is electronic mail. For years, communications experts have considered electronic mail—generally defined as the electronic transfer of written information—to be a tool of tremendous potential. Electronic mail allows an executive such as Coughenour to send messages instantly to employees around the world, far faster than by any courier service.

But the potential of electronic mail has largely been unrealized. Private electronic mail services did only about \$40 million worth of business in 1983, and the few companies with their own internal systems, of which Citicorp is considered a

leader, sent about an equivalent number of messages, estimates Kenneth G. Bossomworth, president of International Resource Development Inc., an electronic mail consulting firm. Growth has been slow because the electronic mail systems have generally required both the sender and recipient of a communication not only to have computers but also to subscribe to the same system.

Industry observers expect that electronic mail will take off with MCI Communications Corp.'s entry into the business. In September, MCI launched an electronic mail service that allows anyone with a computer terminal, or even an electronic typewriter, to send a message to anyone else in the United States. If the recipient does not have a terminal, the message is printed nearby and delivered either by courier or the U.S. Postal Service.

MCI is predicting rapid growth for the system: from 80,000 users today to 200,000 by 1985. And industry experts are inclined to agree. "The MCI entry will transform the industry's revenue picture," said Bossomworth.

With the proliferation of computer terminals in the home and the office, electronic mail could eventually siphon off a significant chunk of both mail and telephone business. In 1982, the congressional Office of Technology Assessment calculated that ultimately at least two-thirds of the Postal Service's annual volume of 110 billion pieces "could be handled electronically." By 1990, the office estimated, more than 23 billion messages could be sent through electronic mail or electronic funds transfer systems. The report predicted that conventional mail volume is likely to peak in the next decade and then decline.

Though the economic prospects for electronic mail may be starting to clear up, the laws covering it remain cloudy in two basic areas: unauthorized entry into such systems and requests by law enforcement officials for access to the records of people's communications held by electronic mail networks, such as MCI. The legal uncertainty underscores the major privacy concern of electronic mail's potential customers, who are worried about competitors reading their internal communications. "The fear [among possible users] is that somebody will get access to the system's central computer and get access to their messages," said computer consultant Walter E. Ulrich, who chairs the new Electronic Mail Association's committee on privacy. Prosecutors have complained that while existing laws can be used against criminals who use computers to commit fraud, no law clearly makes it a crime to break into a computer system to look



In a matter of seconds, Citicorp vice president Richard W. Coughenour sends messages on his Displayphone from his office on Wall Street to bank employees around the world. Although the message is easy to send, it is also easy to steal.

around or destroy information. Some legal barriers are in place. About 20 states have laws addressing unauthorized computer break-ins, and some experts note that if someone sought unauthorized entry into a computer system by misrepresenting himself as an authorized user he could be prosecuted under the federal wire fraud law.

But the electronic mail industry, among other computer users, would like clearer protection. The wire fraud law "was not designed for the problem of trespassing against someone's intellectual or electronic property," said Jack Greenberg, general counsel of GTE Telenet Communications Corp. Telenet runs a private electronic mail system used by 130 companies that was broken into repeatedly last summer, most notably by a group of Milwaukee teenagers using home computers.

Rep. Bill Nelson, D-Fla., and Sen. Paul S. Trible Jr., R-Va., have introduced identical bills (HR 1092, S 1733) that would make it a federal crime to "take something of value" from a computer or to damage the information in it. Nelson's bill has also been incorporated into legislation pending before the Judiciary Subcommittee on Crime that addresses credit card fraud. Both the Nelson and Trible bills, though, still would not make it a crime to enter a computer system and look at the data in it. An aide to Nelson said the bill's sponsors did not believe that should be a federal crime.

While Congress slowly considers these proposed legal barriers to computer break-ins, electronic mail companies have been beefing up their technical defenses. In October, the Defense Department split the 15-year-old ARPAnet, an

electronic mail network run by the Advanced Research Projects Agency, into separate systems for military and unclassified civilian research to further limit access to military secrets. Unlike other systems, the new MCI mail will not allow users to pick their own passwords—which are often no more sophisticated than the name of the user's spouse. Instead the new system assigns passwords that are randomly generated.

The electronic mail operators have also installed systems to prevent would-be intruders from programming their own computers to repeatedly try possible passwords until one clicks. Usually, the systems disconnect a user after three unsuccessful attempts at the proper password. After three such disconnections, the MCI system is programmed to notify the firm's security department.

Citicorp's system has similar security protections. But no system is immune to penetration, said Coughenour, who noted that break-in attempts occur "all the time." The ultimate defense, he said, can only be to keep sensitive information out of the electronic mail system. "Users of the system understand it and know what to put on it," he said. Anyone breaking into Citicorp's electronic mail, he said, would find information of "only minimal" business value.

Even less clear than the law on breaking into an electronic mail system are the legal standards for access by law enforcement officials. For investigators, electronic mail records could be an extremely valuable source of information. "Electronic mail is tremendously attractive to people who are engaged in investigations," said attorney Plesser. "I think law enforcement officials are going to be

come more and more interested in electronic mail records."

Certainly electronic mail networks will contain a wealth of data about the communications of their users. Telenet holds in its computers for anywhere from one day to two weeks copies of messages sent through the system. MCI plans to hold copies of the messages for six months, in case questions arise about billing or customers accidentally erase their messages.

Just the fact that MCI's computer capacity will enable it to hold the messages it transmits for six months makes "some customers nervous," said Marilyn M. Mouly, vice president for marketing of MCI Digital Information Services Corp., the subsidiary that runs MCI's electronic mail system. "When you mail a letter with the Post Office, they don't Xerox it. Generally people see us as carrying messages, not keeping a copy."

There are clear rules on when ordinary mail sent through the Postal Service can be opened. Most correspondence can be opened only after a search warrant is obtained. When law enforcement officials want the Postal Service to tell them from whom a specific individual is receiving mail, they request a mail cover from the chief postal inspector. Under regulation, the inspector is supposed to approve requests only for the investigation of a felony, the location of a fugitive or a national security investigation. In 1983, the Postal Service approved 6,892 mail covers, up 56 per cent from a decade ago. Postal Service officials say these same rules would apply to mail sent through the Postal Service's electronic mail system, known as E-COM.

But the rules for access to privately transmitted electronic mail have not been established. "There is little, if any, legal protection for message information in the hands of private organizations," said Rand Corp. computer security expert Willis H. Ware in recent congressional testimony. In an interview, Ware said he was aware of no law that would prevent a private firm from releasing electronic mail records to police agencies—or anyone else—merely upon their request.

Both Telenet and MCI said they would not release the information to law enforcement officials on request alone and would require a search warrant or a subpoena. But those are voluntary decisions subject to change, and some in the industry would like to see clear legal standards. "It certainly is a gray area of what kind of protection a company has from federal government intrusion," said computer consultant Ulrich.

Similarly, there are no laws governing requests by police officials for the records of the traditional courier services, such as Federal Express. Federal Express attor-



Ronald L. Plessner, former general counsel of the Privacy Protection Study Commission: "Our laws have not kept pace with the [new computer or communications] technology."

ney Elizabeth McKanna said the firm generally would require a subpoena before releasing records, but in some cases, such as the investigation of a bank robbery, might not. "It certainly is not illegal for us to provide them with information," she said.

ELECTRONIC BLINDSPOT?

Also in dispute among experts in the field is whether any law protects an electronic mail transmission or any other communication between two computers, from unauthorized interception while it is in transit.

Two laws govern the interception of telecommunications. Title III of the 1968 Omnibus Crime Control and Safe Streets Act bans the private interception of wire or spoken communications and establishes a process for approval of wiretaps by law enforcement officials. To wiretap a suspect, a federal law enforcement official must obtain the approval of the Attorney General and then a federal judge after demonstrating that there is "probable cause" that the suspect has committed or is about to commit one of a list of specified crimes. Approval is granted only for 30 days or less, and the law allows the judge to require reports on the investigation. These standards are much tougher than the rules governing search warrants or other investigative tools. The second law, the 1934 Communications Act, makes it illegal "to intercept any radio communication and divulge or publish" the contents.

The problem for computer communications arises from the definition of intercept in the crime control law. Though it bans unauthorized interception, the law defines that as "aural acquisition of the contents of any wire or oral communication"—that is, the interception of a voice communication that could be understood by the human ear, as a wiretapper listening to an ordinary phone call would do. But computers utilize non-aural communications that transmit data through a series of digitized bits that cannot be understood by the human ear. For that reason, they are not covered by the law.

No one is accusing the Justice Department or FBI of abusing this provision of the law. Deputy assistant attorney general for the Criminal Division John C. Keeney said in an interview that he has not seen any requests to intercept computer transmissions. But computer users and civil libertarians are concerned that the potential for abuse remains unless computer transmissions are given the same legal protections as telephone conversations.

G. Robert Blakey, a law professor at the University of Notre Dame, who was the principal author of Title III and several other major crime bills when he was an aide on the Senate Judiciary Committee, said that the exclusion of computer communications was not an oversight. "Did we intend to exclude machine-based data? Yes we did," he said in an interview. Congress was worried about wiretaps, whose use had been severely limited by two Supreme Court decisions in the mid-1960s, not about computer privacy, Blakey said. "Congress wasn't prepared to step into computer privacy, and that's the reason we put that word ['aural'] in there," he said. "'Aural' is a neat little word. It simply confines the bill to the consensus that was there" in Congress at the time.

The Justice Department agrees that computers are not covered and that federal officials would not have to go through the extended Title III process to intercept communications between two computers. In a 1978 case, *U.S. v. Seidnitz*, the U.S. Court of Appeals for the 4th Circuit also ruled that non-aural communications were not protected by Title III.

That much seems clear. What is unclear is whether law enforcement officials have to go through any legal process before intercepting computer transmissions.

One answer comes from the courts' rulings on pen registers, devices that record the numbers dialed on a phone, but not the contents of the conversations themselves. In the mid-1970s, American Telephone & Telegraph Co. (AT&T) asserted that the FBI had to receive a Title

III authorization before the company would install pen registers. The FBI argued that an ordinary search warrant was sufficient. In December 1977, a sharply divided Supreme Court ruled, 5-4, that because the pen register was intercepting non-aural communications (the tones that indicate the number dialed) and legislative history made clear Congress intended to exclude pen registers, the FBI did not need a Title III warrant. In two subsequent cases, the Supreme Court and a federal appeals court have held that law enforcement officials did not even need a search warrant to install a pen register. Nonetheless, H. W. William Caming, AT&T's senior counsel on privacy issues, said the firm will not cooperate with pen register requests without a warrant.

But the signals captured by pen registers may be different from other computer transmissions. Because the caller knows that records of the numbers he dials will routinely be held by the phone company for billing purposes, he does not have the same expectation of privacy for that information as he does for the contents of his conversation.

In a transmission of information between two computers, though, the parties would have a reasonable expectation of privacy, several experts said. Legally that expectation puts the communication under the 4th Amendment's protection against unreasonable search and seizure, these experts argue. "In a computer-to-computer transmission, there is a reasonable expectation of privacy, and any interception would be violative of a person's civil rights if done by law enforcement officials without a search warrant," said Caming.

Moreover, a Senate expert on surveillance maintained that the 1978 Foreign Intelligence Surveillance Act, which covers national security wiretaps on foreign agents, limits the ability of federal law enforcement officials to tap non-aural communications. One section of the foreign intelligence law prohibits any federal wiretapping not specifically authorized by statute, he argued; and Title III, because it does not mention non-aural interception, does not specifically authorize it. The foreign intelligence law provides a defense against that ban if law enforcement officials have obtained a court order or search warrant. Other experts, such as Caming, dispute that interpretation of the foreign intelligence law and maintain that it has no bearing on domestic wiretaps.

Justice Department official Keeney said that "if you are going to make any sort of invasion or intrusion, get a court order." It would be his "guess," he said, that law enforcement officials seeking to



Marilyn M. Mouly of the subsidiary that runs MCI's electronic mail system says the fact that MCI's computer capacity will enable it to hold messages it transmits for six months makes "some customers nervous."

intercept computer transmissions would not necessarily need a search warrant—which requires probable cause—but a court order, for which they would have to meet a lesser standard of proof.

But Keeney said he could not make a blanket statement that all interceptions of computer transmissions would require even a court order. "I'm not ready to go that far, no," he said. "You're dealing with a question of expectation of privacy. In some of these areas, there is no expectation of privacy. If you're putting something in the airwaves that almost anyone can pick out, there is no expectation of privacy."

PRIVATE WIRETAPPING

The same kind of uncertainties arise over the laws prohibiting the private interception of computer transmissions. Again, it is clear that Title III's ban on private wiretapping does not protect computer communications, since they are non-aural. But does any other law apply?

Many experts are concerned that there are no clear federal laws prohibiting the private interception of computer transmissions. Other laws could be stretched to cover that situation, said AT&T's Caming: someone intercepting computer transmissions might be prosecuted under the federal wire fraud laws, or under computer protection statutes in the states that have them, and could even face civil liability for the theft of trade secrets. "But," he said, "that is not as strong a deterrent as a specific federal law."

An attorney for a private data transmission company said that the 1934 Communications Act, which bars the unauthorized interception of radio commu-

nications, could protect some of these messages. Before 1968, this law had established the rules for interception of both wire and radio communications, but Congress removed wire communications from its scope with the passage of the crime control act.

Computer messages, though, like other telecommunications, often go through several steps to completion: along local phone wires, through microwave relays and off satellites. The attorney argued that the 1934 act's ban on intercepting radio communications would make it illegal to intercept computer communications during the microwave or satellite, though not the wire, portions of their journey.

At least two appellate court decisions cast doubt on that interpretation. In a 1973 case, the U.S. Court of Appeals for the 9th Circuit ruled that when any part of a communication is carried by telephone wires, the entire communication is covered not by the Communications Act but by Title III. In a 1975 case, the U.S. Court of Appeals for the 5th Circuit rejected the argument that long-distance calls carried over microwave relays were covered by the Communications Act.

AT&T's view, said Caming, is that both the microwave and satellite portions of a telephone communication fall under Title III's definition of a wire communication.

Blakey, though, argues that it is erroneous to assume that courts would come to these same conclusions about the coverage of the Communications Act if faced with a private interception of computer transmissions. In defining wire and radio communications, the courts have gener-

ally been looking for ways to allow evidence obtained by law enforcement officials to be used over the objections of defendants who maintain that it was illegally collected. It is not likely, Blakey maintained, that the courts would allow

it costs more to send an encrypted message. Citicorp uses a simple encryption for its electronic mail and a much more sophisticated system for its electronic funds transfers, whose security is of far greater concern to the bank. Those trans-

security payment records to uncover payments to people who have died.

In one case, during the final months of the Carter Administration, a regional HHS office in Sacramento analyzed its enforcement records to compile a portrait of what it called a "welfare queen" and then ran that profile against a list of county welfare recipients. Those who met the characteristics were singled out for further investigation, though because of staff limits, the office actually investigated only a few of those identified.

Over all, an HHS official estimated, the federal government has undertaken 2,000-3,000 matches, many of which are repeated regularly.

Supporters say that matching is a cost-effective and efficient way to uncover possible fraud in federal programs without creating an undue invasion of privacy. "Of course we have to match," said former privacy commission chairman Linowes. "You have a need for law enforcement, for proper administration in government. You just can't say one thing is completely wrong in most cases."

Critics say that even if each individual use can be justified, the cumulative uses of computer matching can constitute a serious invasion of privacy. Public opposition quickly grounded plans discussed by the Johnson Administration to create a national data bank that would have centralized all the data held on individuals by the government. Matching, said John H. Shattuck, national legislative director of the American Civil Liberties Union (ACLU), accomplishes the same end "through the back door."

Some critics say that matching undermines 4th Amendment protections, since the records of all individuals in a program are searched, not only those for whom program administrators have reason to suspect of a crime. Others, such as Sen. William S. Cohen, R-Maine, worry that in the rush to find waste and fraud, the privacy implications of the growing use of matching are being overlooked.

"As you look at each case, you can make a reasonable case for an exemption from our privacy law," Cohen said in an interview. "I'm trying to say we need to stand back and take a broader view. . . . There is another pressure [besides looking for fraud], more constitutional, more indigenous to our society, which is not being felt at this time: the need to protect privacy in our technological society."

The Massachusetts case demonstrates both the advantages and hazards of matching. In one instance, the state terminated the medicaid benefits of an elderly woman in a nursing home because she possessed assets over the limit. But it was later revealed that her major holding

Computer users and civil libertarians are concerned there is potential for abuse unless computer transmissions are given the same legal protections as telephone conversations.

private wiretappers to use those definitions to slip through a blind spot in the law and escape punishment. Wiretappers would face liability under either the wire fraud statute or the Communications Act, he said.

Nonetheless, Blakey, like many other experts in this area, said he would "applaud any effort by Congress to take a look at the specific protections" available for computer communications. Several legislators already are. Kastenmeier's staff has been looking at the issue, and Sen. Walter D. Huddleston, D-Ky., a member of the Select Committee on Intelligence, has indicated he would support legislation to protect non-aural communications.

Whatever the state of the law, catching private wiretappers is not easy. No one has a good estimate of the amount of private wiretapping that is going on, said computer security expert Ware.

Although it is technically easy to intercept microwave transmissions, most would-be wiretappers are deterred from seeking to tap the phone company's network that way because of the high cost of sifting through the mass of messages flowing through the microwave links to find the ones they want. (That is not a problem if the wiretapper is looking for the messages of a single company, such as Citicorp, that are carried along a private network.) Usually private wiretappers seek to intercept messages by breaking into local phone lines near the subject, say security experts.

The Carter Administration, which was concerned about the Soviet Union's intercepting microwave transmissions with equipment in its offices in New York, San Francisco and Washington, undertook a series of steps to increase the security of government communications and pushed private companies to protect their communications through encryption, or encoding of the information. Only about 100 companies, mainly financial institutions worried about embezzlers sending phony messages to transfer funds, encrypt their data communications, said a government official.

Firms have resisted encryption because

it costs twice as much to send as the electronic mail messages.

To some extent, new telecommunications technology itself will offer greater protection against interception. More messages are being sent through packet switching technology, which breaks up a communication into separate pieces and routes each piece along whatever space is free on many different communications paths. The result is that a single message may travel on several different paths, and the bits of information following each other on any single path may be unrelated.

AT&T is changing its current system under which a phone conversation follows on the same communications path as the tones that indicate which phone number has been dialed. That system allows wiretappers to program their computers to look for a specific phone number and then begin recording. Under the new system, which is already in place in half of the interstate network, the tones will travel along a different path from the communication itself. Neither of these offer insurmountable problems to the most sophisticated wiretappers—such as the Soviet Union—but they do make the job harder, communications experts say.

COMPUTER MATCHING

Another area where privacy laws are fuzzy is the use of computer matching, a technique used by government investigators to find fraud. Matching takes many forms, but generally it entails the computer comparison of two lists to find anomalies that would indicate fraud.

In Massachusetts, for example, state welfare officials have compared recipient roles for welfare, medicaid, food stamps and other benefit programs against account records in the state's banks to find beneficiaries with more than the legal limit in assets. The Health and Human Services Department (HHS) has matched welfare rolls against lists of federal employees and compared the employee lists with the list of those who have defaulted on student loans. The department's Project Spectre compares medicaid and medicare death files to social

was a funeral bond, which is permitted under the rules. Since then, the state has made procedural changes in the match program that have alleviated many of the concerns of advocates for benefit recipients. And the state estimates it has saved at least \$5 million by finding 2,000 benefit recipients with assets over the legal limit.

The law governing the use of federal records is the 1974 Privacy Act. The act generally prohibits the dissemination of government records outside of the agency that collected them. But because of a concession made to get the bill through, the law allows agencies to exchange records for "routine use." That is defined as a purpose "compatible" with the one for which the records were originally collected.

The routine use exemption has become the legal basis for matching. Matching critics say that the intent of the privacy law was to prevent records from being passed between government agencies on a regular basis. "I don't think there was anything more clearly thought about than that," said James H. Davidson, a former Senate aide who helped draft the law. "That is what the Privacy Act is about." When the Carter Administration proposed its first match of federal employees against welfare rolls, the Civil Service Commission initially resisted on the ground that such use of employment records would violate the act.

But eventually, the commission backed down. And Shattuck said that whatever the intent of the Privacy Act's drafters, the language of the statute makes it virtually impossible to challenge a match in court. "I think any match that uses information that is not clearly in the public domain is a violation of the Privacy Act," he said. "Unfortunately, the act is written in such a way as to make that extremely difficult to prove in a court of law."

Christopher C. DeMuth, administrator of the Office of Management and Budget's (OMB) office of information and regulatory affairs, which is charged with ensuring federal compliance with the Privacy Act, agreed that the law does not offer clear guidance on what matches might be inappropriate. Congress, he said, "had to settle for a formulation that is sometimes attacked as too nebulous." But he said the fears about matching have proven unfounded. "The fears that these matches would be used as fishing expeditions have not come to pass," he said in an interview. "The matches have been quite narrow and related to highly plausible concerns about fraud and abuse."

With budget cuts forcing welfare program administrators to trim benefit rolls, few legislators have expressed much con-



Sen. William S. Cohen says there is a "need to protect privacy in our technological society."

cern about the privacy implications of matching. The House Government Operations Committee recently criticized OMB for not monitoring agency compliance with the Privacy Act. Cohen held hearings in December 1982 on matching and is planning hearings on matches conducted by the Internal Revenue Service, including the use of mailing lists purchased from private firms to look for tax evaders and the growing use of IRS data for nontax purposes such as aiding in the collection of student loans. Recently, the National Senior Citizens Law Center won a case in the U.S. District Court for the District of Columbia stopping a proposed Social Security Administration program that would have required recipients of supplemental security income benefits to disclose their tax returns.

But over all, said Cohen, there is "not a whole lot of interest" in the subject among his colleagues. "The potential for abuse is there," he said, "although it does not seem imminent to most individuals."

That assessment does not surprise Robert Ellis Smith, who has been watching these issues for almost a decade as publisher of the *Privacy Journal*. "I think legislation often gets enacted by anecdote," he said. "And the anecdotes are often more compelling on the side of access."

CONTROLLING RECORDS

For records held by the federal government, the Privacy Act establishes minimum standards that allow individuals to

see and correct their own records. But for the vast majority of records held by private firms, there are no laws. Congress has passed legislation placing some limits on the use of records held by banks, credit bureaus and educational institutions. And last year, as part of cable television legislation, the Senate voted to limit the use of information about subscribers without their consent. Similar provisions are contained in the House version of the bill, which has passed the House Energy and Commerce Subcommittee on Telecommunications, Consumer Protection and Finance. In full committee, it is likely that efforts will be made to revise those standards to reflect objections from the cable industry and advertisers who sell product on cable.

But generally, Congress has paid little attention to the central thrust of the privacy commission's study in the mid-1970s. The commission argued that basic principles were needed to govern data collection and use of information about individuals held by institutions and to ensure that individuals could see and correct information about themselves. Since that report, only the legislation governing bank records, which is considered weak by many privacy experts, was enacted. Another major proposal dealing with medical records failed.

Like the issues of electronic mail and protection of computer transmissions, the use of privately held records has not yet attracted sustained political attention. "Our concepts involving information privacy haven't even begun to be addressed," said former privacy commission chairman Linowes. "We don't have a public policy on information protection and privacy."

Such a policy would not require limiting the advance of computer and communications technology. Linowes and other experts argue, but would establish principles of law. "The technology makes it easier both to collect and disseminate personal information without the person's knowledge," said Richard M. Neustadt, who worked on privacy issues as an associate director of the domestic policy staff in the Carter Administration and is now the senior vice president of Private Satellite Network Inc. "But that's nothing new. We've had personal records existing in file cabinets for a long, long time. All the computer does is put more records in and make it easier to get at."

"What we're seeing is old problems made more complicated, more real. But they are solvable. I think you can have your cake and eat it too, if we write some good rules about this stuff. Unfortunately, there doesn't seem to be much interest in doing that in Washington now." □

[From the New York Times, Mar. 13, 1984]

IRS SEEKS LINKS TO COUNTY COMPUTERS IN TEXAS TO FIND DEBTORS

(By David Burnham)

WASHINGTON, March 12.—An Internal Revenue Service office in Texas is seeking to establish electronic links with the computers of 80 counties that will provide it instant access to local records concerning property taxes, voter registration and automobile ownership.

The I.R.S., which already has established such a link with one major county in Texas, said it would use the information to track down individuals who had failed to pay their taxes.

Spokesman for the revenue agency in Dallas and Washington said the Texas project had not yet been attempted in other sections of the country, and there are no plans for expansion at this time.

The project raises the question of whether the impact of information changes when it can be instantaneously assembled, according to critics of the plan. Although the information that will be transmitted to the service by computer terminals has long been publicly available, the project has generated opposition from conservative Texas politicians and a spokesman for the American Civil Liberties Union.

The criticism voiced by several members of the commission that governs Tarrant County, the area around Fort Worth, was so sharp that two weeks ago the I.R.S. withdrew its proposal to establish a direct link with that county's computers.

OFFICIALS FEAR EFFECTS

"This was just another extension of the drive by the Federal Government to gradually increase its power over local government," said B.D. Griffin, a Tarrant County commissioner.

Secretary of State John Fainter raised another objection, saying, "The specter of the I.R.S. having direct access to voter registration records may intimidate those persons considering registering to vote."

But Glenn Cagle, the director of the revenue service district that covers 143 counties of northern Texas, defended his plan as a way of reducing the costs of gaining information the Government could obtain anyway and said he was surprised by the opposition.

"I am not going to speculate on the motives of the critics," he said. "But the fact is this is an election year."

An I.R.S. spokesman in Washington, Scott Waffle, said he too was surprised by the adverse reaction. "All that is happening down there is an effort to improve the Government's efficiency by lessening the cost of obtaining information that always has been available to anyone who asks for it," he said.

Mr. Waffle added that the project was not the result of a national directive to the I.R.S.'s 63 districts and that as far as he knew was not currently being pursued in other regions.

The district that is moving to develop direct computer links has its headquarters in Dallas. In 1982, the individuals and businesses within its borders filed 4,858,821 of the 171 million tax returns the agency received.

Last summer, Mr. Cagle wrote each of the counties requesting information about the extent to which their records were computerized and whether they would be interested in the project to give the I.R.S. direct access to them.

Marlene Gaysek, an agency public affairs official in Dallas, said the district was negotiating with 80 of the counties and expects to complete arrangements with 20 of them soon.

According to the contract that has been signed with Dallas County, which has 1,644,000 residents, the revenue service will have a county terminal in its Dallas office that will allow its 2,000 employees to make nearly instantaneous checks about the property owned and the property taxes paid by every person in the county; the name and address of all persons with a registered vehicle; the make, year and weight of that vehicle, and the name and address of every registered voter.

Although the I.R.S. requested access to all the data in the voter registration files, the Dallas County commissioners ruled the agency could not obtain the dates of birth, Social Security numbers or telephone numbers of individuals.

Miss Gaysek said the computer links would save the agency about \$200,000 a year because lower-paid clerks, rather than field agents, would be able to gather information, and travel costs would be avoided.

She said the district office would not use its computer access to compile complete new lists of all individuals living in an area that then would be matched against computerized lists of taxpayers.

"There has been a real misunderstanding," she said. "We're not taking wholesale lists for computer matching purposes, we are using our direct access to track individual taxpayers. We need this detailed information when we file a tax lien against someone on check to make sure a taxpayer's financial statement is correct."

PRIVACY ISSUE RAISED

James C. Harrington, an attorney in the state office of the A.C.L.U. in Austin, said that even though the information the I.R.S. would receive by computer was public, the use of county data conflicted with one of Congress' chief goals in protecting Federal records; a guarantee in the Privacy Act that the information an individual provides the Government for one purpose will not be used for another without the individual's permission.

"We generally oppose this kind of cross computerization because despite what any agency says, history tells us that the information the I.R.S. is collecting will be compiled into a giant centralized data base," he said. "History also teaches that we have to develop appropriate legal restraints on all Government agencies."

Tony Bonilla, the chairman of the National Hispanic Leadership Conference, said: "The bottom line is that this project is not necessary. The I.R.S. already has enough information about every taxpayer."

[From the New York Times, Apr. 8, 1984]

U.S. AGENCIES TO GET DIRECT LINK TO CREDIT RECORDS

(By David Burnham)

WASHINGTON, April 7.—Federal agencies will be able to obtain direct 24-hour-a-day computer access to Americans' credit records under contracts now being negotiated by the General Services Administration.

The Government has almost completed arrangements for establishing direct electronic links, between about 100 Federal agencies and seven major credit reporting companies that keep records on more than 100 million individuals and companies.

The Government already has the legal right to obtain credit information before it grants loans. Once the links are in place, agency personnel could examine, almost instantaneously, the current status of bank loans, liens, divorce records, and department store, oil company and credit card accounts.

DETAILS OF FEDERAL LOANS

In addition, Federal agencies will give the private credit reporting companies details about loans made to individuals or companies by such agencies as the Department of Education or the Small Business Administration.

Authorization for the new links was contained in legislation approved by Congress in 1982, and the sharing of information between the public and private sectors will be carried out under many of the guidelines established in the Fair Credit Reporting Act of 1968.

Robert Ellis Smith, the publisher of The Privacy Times, said Thursday at a House hearing that arrangements for the links were almost complete.

MOST SHOCKING ASPECT

Mr. Smith, testifying before the House Judiciary Subcommittee on civil liberties, said "the most shocking aspect" of the exchange was that the credit reporting business "has a poor reputation for maintaining the accuracy of its information."

He said one of the major credit reporting companies, TRWs Inc., estimated that a third of the million people who each year demand to see their records "challenge the information they see in their files."

An official in the Office of Management and Budget, John F. Donahue, confirmed that the contracts establishing the new communication networks were nearly complete. He said the system was an important new weapon in the Government's arsenal against waste and fraud in Federal programs.

Mr. Donahue said that under new guidelines published by his agency last summer, all agencies that grant loans to individuals or companies, or that sign con-

tract with corporations, are required to make credit checks in which a wide range of personal information will be made available to the Government.

Law-enforcement agencies have more limited access to the detailed credit records. According to Marvin Kaplan, a spokesman for the Association of Credit Bureaus, such agencies as the Federal Bureau of Investigation can obtain only names, addresses, former addresses and places of employment, unless they get a court order.

Five of the credit reporting companies collect computerized information about the credit of individual Americans and two collect similar data on companies. The information, generally maintained in large computers and updated monthly, is sold to merchants, banks and other lenders.

REVENUE SERVICES TEST PROTESTED

While the credit information has been used by Government agencies in the past, the combination of the new budget office regulations and the development of the computerized links are expected to make such checks far more extensive.

Also at the Thursday hearing, Alexander C. Hoffman of the Direct Marketing Association testified against a test by the Internal Revenue Service to determine whether national mailing lists can be used to identify individuals who have not paid their taxes.

[From the Christian Science Monitor, Apr. 17, 1984]

WHO'S SNOOPING AND HOW? U.S. AND U.S.S.R. "PEER INTO MIST"

(By Peter Grier)

WASHINGTON.—Pretending to be a Soviet eavesdropper, I peer into the purple mists of northern Virginia, searching for the Pentagon.

I am standing on the roof of an apartment on upper Wisconsin Avenue, one of the highest spots in Washington. Next door, the spindly legged frame of the new Soviet embassy is just emerging from morning shadows.

From this vantage point, two things about the half-finished embassy quickly become apparent: 1. The Soviets will have a great view. 2. Their antennas will pick up more than HBO and "This Week with David Brinkley."

To the south, next to the gray ribbon of I-395, the Pentagon is clearly visible. To the east is American Telephone & Telegraph's (AT&T) Arlington switching station, which sends an electronic beam of phone calls shooting right over the Soviet site. A few blocks north are the towers of the Naval Security Station and Western Union's Tenleytown microwave relay.

The prospect of foreign aeriels in the midst of this electronic interchange illustrates a dilemma of modern telecommunications. Whiz-bang technology makes the United States system the best in the world, say telecommunications experts—but that same technology makes it relatively easy to intercept messages.

The U.S.S.R. from trawlers, trucks, and rooftops, has been listening in on our phone calls for years, say U.S. officials with access to intelligence information.

The National Security Agency, the U.S. government's secretive electronic intelligence arm, scans an unknown amount of US messages headed overseas, according to court records and civil liberties advocates.

Furthermore, it may be perfectly legal for anyone to eavesdrop on computer communications. Experts worry that wiretap law may cover only human speech, leaving the "beedle-de-beep" of computer talk unprotected.

In general, it is the demise of the wire which has made these activities possible. Once, phone calls traveled only paths of copper; today many are shot across country by microwave. Microwave beams can be a third of a mile across, and to catch them, all an eavesdropper must do is hoist small dish antennas in their path. If the beam is an AT&T trunk line, sophisticated computer analysis is then required to unravel it.

Overseas messages bounced off satellites are even easier to grab. With a good dish, satellite traffic can be stolen from anywhere in the U.S. from ships offshore, "even from Cuba," wryly notes a former White House communications official.

Wireless phones are vulnerable, too. If you have a cheap model, neighbors may be able to hear parts of your conversation on AM radio. Last December, police in Woonsocket, R.I., used this eavedrop technique to snare a 19-member drug ring.

All this doesn't mean there are lots of little guys out there listening to your calls. For the most part, only nations indulge in extensive electronic eavesdropping.

The Soviet Union is the most notorious example. Their buildings—from the old Embassy on 16th Street here, to the United Nations Mission on 67th Street in New York, to the West Coast consulate on top of a San Francisco hill—are topped with forests of antennas. From these rooftops and elsewhere, the U.S.S.R. has been listening in on U.S. phone calls for at least a decade, say government and academic sources.

They are probably after more than military secrets. "Department of Defense [communications] will be encrypted," says an official who worked on the issue for the Carter administration. "The problem is that sensitive private-sector information is vulnerable."

Conversations pulled from the sky have likely helped the Soviets in grain-contract negotiations, for instance, says this source. Their Glen Cove, N.Y., weekend lodge is well-positioned to listen in on Long Island's defense industries. The San Francisco consulate is thought to hide equipment trained in Silicon Valley.

Defensive measures have been taken since the eavesdropping was first discovered. U.S. government communications have been rerouted underground; important defense contractors have been outfitted with government scramblers. AT&T now beams most microwaves in a way that is much more difficult to unravel, says Willis Ware, a Rand Corporation communications expert.

But the U.S.S.R., at the same time, has been updating its interception gadgets. Overall, "the situation is more or less the same," claims a congressional aide with access to intelligence information.

Other nations probably have electronic eavesdropping equipment in the U.S. though not on the same scale as the Russians. The U.S. itself, however, has high-tech ears that put the Soviets to shame.

The National Security Agency (NSA), the US electronic intelligence arm, has six times the number of employees of the Central Intelligence Agency (CIA), according to congressional estimates, and has giant antennas from suburban Washington to Pine Gap, Australia.

Most of these ears are trained on other nations, straining to pick up chatter between Soviet pilots or data from Chinese missiles. But some are turned inward to monitor U.S. phone calls and telegrams headed for other nations.

NSA dishes in Sugar Grove, W.Va., can eavesdrop on a nearby COMSAT post that handles half of all U.S. international satellite communications, says James Bamford in his book "Puzzle Palace." NSA installations in Maine, Washington State, and California have similar purposes, he claims.

The NSA sweeps up vast numbers of messages headed overseas from the U.S., according to records from a 1982 court case on use of the agency's intelligence. High-speed computers then rifle through this raw data at leisure. When they stumble across a keyword ("Khomeini," perhaps) that means the message might be useful, it is printed out for further study. Other communications are discarded.

A U.S. appeals court judge, in the context of the '82 suit, did not find this activity illegal. But some congressional aides and civil libertarians feel the NSA impinges on citizens' constitutional rights, as the agency's methods inadvertently filter millions of innocent messages.

"The intrusion is no less serious because it's so quick, or because no trace is left, or because no human is involved," says David Watters, an electrical engineer and former consultant to the CIA.

The NSA's power has been abused in the past: Between 1945 and 1975, under "Operation Shamrock," the agency was given copies of almost all telegrams sent overseas. During the Vietnam war era, the NSA listened to conversations of Jane Fonda, Dr. Benjamin Spock, and others on a "watch list" of 1,650 protesters.

Today, "the NSA does not target the communications of U.S. citizens," a former NSA director, Vice-Adm. Bobby Inman, said in an interview.

"The provisions are also in place to suppress any potential for saving a 'watchlist' of knowledge that's incidentally acquired," he added. "There is not, in fact, a danger of Big Brother turning to listen to the communications of its citizens."

There may be a danger in the U.S. however, of unwanted ears listening in on the communications of computers. The 1968 Crime Control Act, which governs non-national-security wiretaps, prohibits "aural acquisition" of telecommunications. In other words, it's illegal to intercept a communication you can hear and understand.

But as anybody who's ever listened to computer "speech" knows, you can hear it—but you can't understand it.

Ron Plesser, counsel to the 1977 Privacy Protection Commission, says that means that it may be perfectly legal to eavesdrop on computers. "It's a real issue," he says, "although I don't think it's that hard to fix."

This glitch is a good example of how quick-footed innovation often outflanks efforts to control and protect it.

"These technological advances happen so quickly that the normal process our government and society uses for adjusting to change doesn't have time to take effect," says Arthur Bushkin, a former Commerce Department information policy official.

[From the Christian Science Monitor, Apr. 18, 1984]

WIRETAPS: IS THERE ENOUGH SUPERVISION?

(By Peter Grier)

HAUPPAUGE, NY.—"Keep out" is penciled on the battered door. We knock before entering, to make sure no one's inside.

The room looks like a junior high school teachers' lounge. It is windowless, with aged chairs, a Cyclops eye of a clock, and a carpet that was once orange. Along one wall stretches a counter that would be perfect for eating lunch—if you moved all the tape recorders.

"I wouldn't let you in if they were listening," says Ray Perini, chief of the Suffolk County narcotics bureau.

This, in fact, is a wiretapping lounge. From here, Suffolk County detectives with headphones and Superscope recorders listen in on suspects' phone calls. It's amazing, they claim, how loose-lipped criminals can be.

"They say stuff like, 'You talk, my phone is tapped,'" says Mr. Perini.

After declining steadily through the late '80s, the use of wiretaps in law enforcement is again on the rise. In 1982 (the last full year for which data is available) court-approved taps were up 22 percent, to 578. Preliminary figures show the numbers continued to climb during last year.

Yet wiretaps and bugs are powerful, potentially dangerous tools. The average tap hears 58 people, both guilty and innocent. "Videotapping" with tiny cameras can leave no place to hide.

Are investigators with headphones trampling on constitutional rights?

"Wiretap law is a disaster," claims John Shattuck, national legal director of the American Civil Liberties Union (ACLU).

Over 50 years ago, United States Supreme Court Justice Oliver Wendell Holmes called police wiretapping a "dirty business." Even today, 23 states forbid their police departments from using taps and bugs.

But to officials who use it often, electronic eavesdropping is an invaluable weapon in the war against crime.

Take the Federal Bureau of Investigation. Most of the jump in eavesdropping has been caused by the FBI, in its pursuit of drug rings. Fighting the new wave of such criminal enterprises, says FBI chief William Webster, requires greater use of "sensitive" techniques.

"I feel very comfortable using wiretaps, if guidelines are carefully supervised," Mr. Webster said in a recent interview. "They have been enormously effective. There's still a kind of carelessness where telephones are concerned."

In Suffolk County, on the eastern half of Long Island, there are apparently a lot of careless criminals.

Suffolk prosecutors installed more wiretaps in 1982—30 of them—than any other US county. According to federal records, about one-third of the 595 conversations these taps intercepted were "incriminating."

"You know that scene in the movie 'Annie Hall,' where Woody Allen sneezes and blows \$2,000 worth of cocaine all over the floor?" says Dave Freundlich, Suffolk assistant district attorney. "I heard that really happened once."

Often, says Mr. Freundlich, suspects know they are being tapped, and try to disguise the nature of their conversations. But their codes are sometimes less than cryptic.

"One guy will say 'Bring me a tire. A whole tire,'" says Freundlich, "and then the other will ask, 'Do you want the big tire, or the little one?'"

Long Island's ragged shoreline is a haven for drug smugglers, and narcotics suspects account for most of Suffolk's wiretaps.

Without electronic help, claim county prosecutors, their arrests would reach no higher than street dealers. With taps, they say, they are getting the top dealers in the county—such as Ronald DeConza, convicted in '82 of distributing cocaine.

Assistant district attorney Freundlich insists that Suffolk detectives strictly follow federal wiretap laws. But he admits that the taps are "a big drain on our resources."

Indeed, wiretaps are as expensive as a Mercedes sedan. The average cost of a tap (including both equipment and manpower) was \$34,000 in '82, according to the administrative office of the United States Courts.

And that, say critics, is a lot to spend for something they consider both a dangerous intrusion on privacy and unnecessary.

"They should yank them all," grumbles Herman Schwartz, a law professor at the American University.

Wiretaps are powerful vacuums that suck in the words of both criminals and innocent phone users. Between 1977 and 1982, federal taps overheard some 260,000 people—the vast majority of them innocent of any wrongdoing. Officials must turn off their equipment if a chat is not suspicious. But even a few seconds of eavesdropping, say civil liberties advocates, constitutes an invasion of privacy.

"They are inherently intrusive. It's analagous to searching all the apartments in a building, on the grounds that one may have something in it," says the ACLU's Mr. Shattuck.

Wiretaps are also sometimes unconstitutional "fishing expeditions," say civil liberties advocates. Official reason, "Let's put a wire on this nasty guy and get him for something," critics say.

On a less theoretical level, eavesdropping critics argue that the technique is simply ineffective—that prosecutors, after they cast their electronics net, haul in only a few small criminals.

Over the last five years, wiretaps have led to the conviction of an average 900 criminals annually. The majority of these are small-time gamblers and street dealers, says Herman Schwartz of American University.

"If I was a Mafia figure, I would make darn sure never to say anything incriminating over the phone," Shattuck adds.

And judges probably don't watch over wiretaps as closely as they should.

The courts are charged with making sure officers follow that wiretap standards set in the Omnibus Crime Act of 1968.

Eut "the truth is, on the state level, oversight is difficult to achieve," admits a law-enforcement official who asked not to be named. "How would you like to leaf through hundreds of conversations?"

The technique of wiretapping itself has changed little in the years since the Omnibus Act was passed. "Wiremen" still find the phone box near a suspect's home or apartment, take a short wire with clips on each end, and connect the tapped line with one running back to the prosecutor's office.

Detective then spend eight-hour shifts in bored seclusion, waiting for the tapped phone to ring.

But technology, since 1968, has not been standing still. Officials now use some gadgets the law did not foresee, such as electronic "pen registers," which record numbers dialed, not conversations, allowing police to discover a suspect's contacts.

"Videotapping," in which small cameras watch suspects, is a still-small, but particularly Orwellian new development not covered by the law, says one congressional aide.

If your phone is tapped, you can keep your mouth shut. But if there's a camera in your ceiling, there's nothing you can do, short of hiding under the table. A federal district judge, in 1980, called videotapping "extraordinarily intrusive," although he did not throw out camera-obtained evidence.

The use of bugs and phone taps raises difficult questions about both the need for security and rights to privacy.

It is a subject fraught with tensions.

"Electronic surveillance is the only way to get the big guys," sums up Michael Goldsmith, counsel to the New York organized-crime task force, "but its use needs periodic review."

[From the Christian Science Monitor, Apr. 19, 1984]

AUTOMATIC TELLERS, ELECTRONIC MAIL RAISE PRIVACY CONCERNS

(By Peter Grier)

ANNAPOLIS, MD.—I am 50 miles and one state away from home, and in desperate need of money for lunch.

After all, this antique Chesapeake Bay town is famous for seafood, as well as sailing. Packs of Naval Academy cadets pass in front of me, enjoying crab cakes, oysters, and steamed clams. Their white hats look like dinner plates worn at a rakish angle.

So I slip my bank card into an automatic teller on West Street (laid out in 1696). Instantly, my request for \$20 is beamed to Baltimore, where a bank computer realizes I'm an outsider. It throws my query to Dayton, Ohio. A computer "switch" in Dayton checks with my Washington-area bank, then tells Baltimore it's all right to give me money.

In 10 seconds, thanks to an electronic banking network, I have cash for a crab sandwich—and a computer in Dayton knows I have skipped out of the office on a sunny, early spring afternoon.

Today, magic webs of computers are rapidly easing many of life's little tasks: getting cash, shopping, sending messages. But at the same time, these webs are hauling in vast amounts of personal data on Americans.

We must keep a careful eye on the rise of automatic banking, electronic mail, and other systems, say experts, if our privacy is to remain protected.

"As a byproduct of the evolution of technology, we are developing a network of surveillance capability," says Arthur Bushkin, who was in charge of President Carter's privacy initiatives, "although it's not out of any malicious intent."

The institutions that run computerized transaction networks all pledge to fiercely guard their customer's data. Yet gray areas in the law, say congressional aides and communications lawyers, may make these actions legal.

Your boss, spouse, or a credit agency could track your movements with the use of electronic banking records. No federal law bars banks from divulging this information to third parties.

If you use electronic mail, law-enforcement officers might be able to read your messages without a warrant. Search warrants are needed to open letters carried by the United States Postal Service.

Subscribers to two-way cable television may find that opinions they register are sold to, say, political parties, with their names attached. Currently, the only laws protecting two-way cable data are state statutes in Illinois, Wisconsin, California, and Connecticut.

Back at the dawn of the information age, when computers took up the floor space of a hockey rink, civil libertarians feared the coming of the Big Box—a giant computer compiling data on everyone in the U.S.

Instead, during the last 20 years little computers have learned to chatter back and forth, over communications links of unbelievable sophistication.

This gift of speech has made possible computer networks that today handle such tasks as reserving plane seats and approving checks. Decentralized, fast, hungry for data, these webs are far more than mere automated clerks, say those who follow privacy issues.

"More information is being maintained on individuals. It's being more centralized. It is more accessible and available," says Ron Plesser, a Washington, D.C., lawyer who was counsel to the 1977 federal privacy commission.

Today, the computers that know the most about us are probably those that handle financial tasks: electronic tellers, credit-card checking machines, and check authorizers. Besides knowledge of how much money we have in the bank, these systems know where we are depositing our paycheck, or paying \$150 for clothes—at the very moment we're conducting the transaction.

And money computers will be even more knowledgeable in the years ahead, as networks grow and combine to provide more services. Soon, for instance, American Express cardholders will be able to charge calls on specially equipped AT&T phones; eventually "debit" cards are expected to link banks and retailers by automatically siphoning cash from our accounts as we make purchases.

"The computer can develop a data base on your preferences: He likes to shop at this store, etc.," says Art Bushkin, now a telecommunications consultant. "It has time data. You can program it to behave preemptively: The next time Bushkin appears within the computer's scope, print out a message for the FBI [Federal Bureau of Investigation]."

Bank officials react indignantly when asked whether they might show this data to outsiders. Most financial institutions have explicit policies on protecting the privacy of their depositors.

But it is only the institutions' good will that guards these secrets, say privacy experts. The laws protecting financial records are very limited, they claim. If the federal government asks to see your bank files, the 1978 Right to Financial Privacy Act

requires that you be notified. If a private party asks for them, it's perfectly legal for the bank to hand over the data without saying a word.

And if you think such things never happen, remember that Bob Woodward and Carl Bernstein, in pursuit of the Watergate story for the Washington Post, found California lawyer Donald Segretti's credit card records to be a rich source of information.

A Congressional Office of Technology Assessment study concludes that the need "for more comprehensive electronic funds transfer privacy protection . . . are still largely unmet."

If anything, there may be even less legal protection for message transmission systems such as electronic mail.

The electronic-mail business, long more promise than performance, is now shifting into second gear. Private firms did about \$40 million worth of business last year, and in September MCI Communications launched its ambitious MCI Mail service.

Yet these ethereal messages, which flit from computer screen to computer screen, are more vulnerable than old-fashioned letters in several respects.

For one thing, some clever users of home computers have managed to break into the networks. Last summer, a gang of Milwaukee teens repeatedly romped through GTE Corporation's Telenet system.

No law explicitly makes this illegal. "It's a very large gray area," says Walter Ulrich, a computer consultant and head of the Electronic Mail Association's privacy committee.

For another thing, both law officers and private third parties might be able to read your messages without your knowledge. MCI, GTE, and other electronic-mail companies all say they will staunchly defend their subscribers' privacy. No law, however, prevents them from voluntarily surrendering your mail.

"Chilling, isn't it?" says Mr. Ulrich.

But it is still another type of computerized network that may have the greatest potential for invading our privacy: two-way cable TV.

Such systems promise to bring a world of services into our family rooms, via color TV. Futurists have long predicted that we will eventually be able to bank, shop, and express our opinion over interactive cable channels.

If so, we will be entrusting cable companies with huge chunks of data about ourselves: buying and viewing habits, perhaps even political and social opinions.

"This sensitive personal information is a valuable commodity which cable companies can sell to . . . interested buyer in order to finance their corporate growth," charges John Shattuck, national legal director of the American Civil Liberties Union.

No federal statute covers the issue. Four states, however, have passed laws prohibiting cable firms from disseminating individualized data. Two more—New York and Maryland—are considering similar laws.

The industry is sensitive to the problem. Warner-Amex Cable, which operates the QUBE interactive system in seven cities, subscribes to privacy code that was the model for several of the state statutes.

Of course, all these systems—two-way cable, electronic mail, and electronic banking—promise great benefits. Privacy experts say they simply want to see laws prohibiting misuse of the networks.

And "we should leave things flexible enough for the people who will want to continue the old ways," such as paying cash for gas, adds Robert Smith, editor of Privacy Journal.

Washington seems only mildly interested in the impact of computer systems on privacy. The House judiciary subcommittee on civil liberties, headed by Rep. Robert Kastenmeier (D) of Wisconsin is holding a series of hearings on the issue. The Commerce Department's National Telecommunications and Information Administration no longer works extensively on privacy.

"Do we as a society accept this evolution [of technology] and its implications passively?" asks communications consultant Bushkin. "Or do we discuss it and decide whether we like the way it is?"

[From the Christian Science Monitor, Apr. 20, 1984]

COMPUTERS NOW PRODUCE CIPHER AS TOUGH AS 6-INCH ARMOR

(By Peter Grier)

RESTON, VA.—"DzX&N8s," says the secret message. "W@0yKlc:\$* Sdfth".

Lapsing into a daydream, I wonder what it could possibly mean: Does McTavish know about the letters of credit, and the carpet dealer in Rabat? If so, then Diane is in danger. Why did the Land Rover have to break down? Cairo will be furious. . .

Larry Conner of Analytics Communications, breaking my reverie, points to the computer screen in front of us.

"This word here is my last name, actually," he says.

We are in a sunny conference room, not a cheap North African hotel. I am being shown Sherlock, a black box that scrambles computer data into dense cipher. It is to paper-and-pencil code what a nuclear submarine is to a dinghy.

"The only known attack is to guess the key," says Thomas Mitchell, and Analytics marketing manager. "There are 72 quadrillion possible keys."

Cryptography—the science of secret communication—is entering a new age.

Gone are the romantic cipher machines of World War II, with their mysterious mechanisms; in their place are powerful microchips. And soon spies and diplomats may not be ciphering's main practitioners. As computer data becomes more valuable, cryptography is moving into the private sector.

"With electronic technology, you can have a much higher degree of security than with ordinary paper files in cabinets," claimed the late Ithiel de Soia Pool, a communications expert at the Massachusetts Institute of Technology.

Take the Sherlock Information Security System. For \$1,995, it drapes secrecy over information transmitted from one computer to another. Messages are unraveled with the aid of a "key," a 56-digit number, all 0s and 1s, which reverses Sherlock's scrambling equations.

Other ciphering equipment on the open market range from the Encryptor, an accessor for home computers that costs a few hundred dollars, to the IBM 3848. For \$58,670, the 3848 will encrypt just about anything.

"Say you've got one of our largest computers," says IBM spokesman Steve Carpenter, "and you wanted everything in it to be in ciphered. The 3848 could do it."

Of course, machines that make communications secret, as if by magic, have long fascinated ingenious inventors.

In the mid-1400s, the Italian architect Leon Alberti perfected a cipher disk that was state-of-the-art technology for 400 years. Thomas Jefferson invented a "cypher wheel" which looked like a rolling pin and served the United States government for a century and a half.

By World War II, governments were encrypting with machines that resembled a cross between a typewriter and a music box. The machines, with such exotic names as "Purple" and "Enigma," used rotating electrified disks to scramble messages.

But with the rise of the digital computer, ENIGMA and its brothers were suddenly obsolete. Changing plain words into ciphertext is, at heart, a mathematical process; and computers do math so fast they produce cipher as tough as six-inch armor.

Computer technology, in fact has reached the point where encryption equations now fit on a single microchip. The Data Encryption Standard (DES), a ciphering algorithm developed by the United States government is available on chips made by Intel, Motorola, Texas Instruments, and many other makers.

These chips are the core of most private-sector encryption equipment. They do not produce impenetrable cipher, but just how much work it would take to uncover these secrets is a matter of some dispute.

A special state-of-the-art computer could crack open a DES-protected message in three days, according to a 1977 Stanford University study. The system's defenders claim such a computer is in fact wildly impractical, and that a more normal computer would need about 3,000 years to unravel a DES transmission.

In any case, DES provides enough protection for anyone short of a government, says Miles Smid, a mathematician with the US National Bureau of Standards.

"They make use of both substitution and transposition [scrambling] encryption," Mr Smid says.

"By using both types, you get a very strong cipher."

So far, commercial encryption is not exactly a hot trend. Analysts estimate that US sales of cipher devices hover between \$200-\$300 million a year.

But as computer networks proliferate and more companies become aware of the value of their electronically-stored data, demand is likely to see a healthy upswing, say communications experts.

"Everyone agrees that the market for cryptography will grow in the next 10 years. What is not clear is how much and how fast," a study by the Harvard Center for Information Policy concludes.

Banks will perhaps be the best customers for the "cryptosystems." Their computers, after all, are electronic vaults that literally store money.

Already, most financial institutions have encryption in their automatic teller machines, to protect customers' access numbers. Electronic funds-transfer (EFT) systems, which shuttle some \$500 billion between banks every day, aren't so well covered, since they're much more expensive to encrypt.

Howard Crumb, an assistant vice-president at the New York Federal Reserve, says only "parts" of banks' daily EFT transactions are in cipher.

"But I hear more and more talk about it, he says. "I see it coming on strong in late 1984. The catalyst was publicity about the 'hackers' who were breaking into computer systems last summer."

In the future, cryptology could also play a crucial role in protecting "information products" such as teletext and Home Box Office. The products would be broadcast in scrambled form; consumers would then purchase a key allowing them access to the data.

Many pay-TV channels already use such a system, points out Victor Walling of SRI International, a think tank in Menlo Park, Calif.

"The problem with a lot of these information products is that if you don't have a key to lock it up, you can't maintain rights to it," Mr. Walling says.

On the whole, however, Walling says there may not be a big private demand for cryptology, at least in the short-run.

"Somebody will have to do a D. B. Cooper with data, before people will really pay attention," he says, referring to the legendary hijacker who parachuted from a Boeing 727 with \$200,000.

Meanwhile, science marches on. University researchers are hard at work on a new type of cipher that may make it even easier for businesses to transmit secret messages: "public key cryptology," or PKC.

Development at Stanford and MIT, PKC uses two keys instead of one. The first can transform plain words into cipher, but can't decode the resulting message. The second, secret key is needed to unlock and read the transmission. Thus a subcontractor of a large oil company, by looking up the company's public key, could send it secret messages—but couldn't read the ciphered transmissions of a fellow subcontractor.

In addition, PKC allows users to add a unique digital "signature" to their transmissions. Eventually, business executives may legally be able to sign contracts by computer, say cryptologists, and exchange certified electronic mail.

Ronald Rivest of MIT, a PKC pioneer, says a computer chip featuring the new cipher will be ready by this fall. It will work more slowly than current encrypting chips, he admits. It thus may be most useful for such smaller applications as protecting information on certain credit cards.

Early versions of PKC have proved vulnerable to cryptologic attack. In 1982, a young Israeli mathematician, Adi Shamir, cracked a Stanford PKC system with relative ease.

But the PKC co-authored by Dr. Rivest, which uses more complicated calculations, has so far remained inviolate.

[From the Christian Science Monitor, Apr. 23, 1984]

SEARCHING FOR PRIVACY IN A HIGH-TECH WORLD: ATTITUDES, NOT TECHNOLOGY, ARE KEY

(By Peter Grier)

CAMBRIDGE, MA.—Congress in 1876 was in an uproar.

The results of that year's presidential election were the subject of bitter dispute. Republican Rutherford B. Hayes and Democrat Samuel Tilden had finished in a virtual dead heat, with cries of fraud on both sides.

So legislators, to help settle the matter, decided to snoop on United States citizens via the latest in high technology—the telegraph. They simply ordered Western Union to turn over 30,000 telegrams from important political figures.

The press was aghast at this invasion of privacy. Western Union's president refused to comply. Congress arrested him and read the telegrams anyway.

No conclusive proof of fraud was found. But the incident shows that "high tech" surveillance is not just a phenomenon of the 20th century. Throughout US history, experts say, the protection of privacy has depended on a mix of factors: technology, politics, and corporate attitudes.

"'Eternal vigilance is the price of liberty.' Some clichés gain currency and stay around, because they reflect basic truths," says Anthony Oettinger, head of Harvard's Center for Information Policy.

Speaking with the steady rhythm of a UPI ticker, Dr. Oettinger leans forward to make his point. Outside, students scuttle across the Harvard Law School lawn.

The leader of a group whose sole purpose is studying the information revolution, Oettinger has "the whole wired world in his hand," according to Harvard magazine. He analyzes some 80 businesses—from cable television to newsstands—for their impact on the flow of data in the US.

Microchip logic, tiny video eyes, and other new-tech gadgets could complicate efforts to shield privacy, he says. But he warns against focusing on the technology itself without scrutinizing society.

"There's no doubt some things are done more efficiently with computers than with goose-quill pens. But I grew up in Europe in the '30s and '40s and saw many friends and relatives carted off by Germans using three-by-five cards," he says. "It doesn't require a computer."

Oettinger is obviously irritated by suggestions that surveillance technology, once born, creates a momentum of its own and will be used for nefarious purposes.

"That's like saying, 'Technology made me do it,'" he says, hands waving. "It's an absurd abdication of responsibility. There is no substitute for a free people, an electorate, whatever, remaining responsible and in charge. I mean, you've got to watch the [offenders], whoever they are."

This does not mean that evil forces lurk just out of sight, ready to wrap the US in webs of surveillance the moment we let down our guard. Compared with both the fictional Oceania of George Orwell's "1984" and to many of today's totalitarian states, privacy in the US is well protected.

It does mean, Oettinger and other experts say, that we must watch for a step-by-step erosion of privacy by government agencies, corporations, and other institutions.

The benefits of new high-tech activities—from the use of computers to detect welfare fraud, to banking with electronic tellers, to on-line criminal information systems—should be weighed against possible intrusive effects.

It's a balancing act," says Oettinger. "The balance is between privacy, an important value, and a lot of other things that we might want."

The US, since its founding, has officially prized privacy. The Fourth Amendments to the Constitution, for instance, guarantees the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. . . ."

But at the same time, US society professes administration for those who have nothing to hide, for men and women whose lives are an open book.

"There is a stress on privacy in the US, and at the same time there is a stress on openness. That helps create a tension, I think, between concealment and revelation," says Sissela Bok, author of the book "Secrets."

Mrs. Bok, a Swedish-born philosopher, is the wife of Harvard president Derek Bok. Her father, economist Gunnar Myrdal, and her mother, peace activist Alva Myrdal, have both won Nobel Prizes.

Her elegant home is near Brattle Street in Cambridge. Outside the library, evening and a late-season snow are falling as she discusses privacy, technology, and secrets.

"With computers, we are in a whole new universe with respect to [protection of privacy]," she says. "In this universe we probably will have to recognize that there are a number of things that can't be exactly private."

The complexity of modern life, in other words, means that data we might prefer to keep private, such as bank balances and health records, won't be under our control.

And control, she says, is what privacy is all about—control over access to information we define as our personal domain. We thus guard our sense of identity.

"We recoil from those who would tap our telephone, read our letters, bug our rooms," Mrs. Bok writes. "No matter how little we have to hide, no matter how benevolent their intentions, we take such intrusions to be demeaning."

When our privacy is invaded, someone or something shows power over us. "If we had no privacy at all, not even the capacity to protect it with secrets, we would be utterly vulnerable," she says.

But privacy for people is not the issue that most concerns Mrs. Bok. Instead, she expresses concern about government secrecy.

The Reagan administration, she feels, has tried hard to slam shut doors to much information. It has become more difficult to pry loose documents through the Freedom of Information Act, she says; Presidential Directive 84, withdrawn after being

blocked by Congress, would have required many officials to sign lifetime secrecy agreements.

"I feel very strongly that there has been a tremendous move towards greater official secrecy in many areas," she says.

Mrs. Bok says the US already has far too much secrets. She cites studies saying that many things labeled "top secret" are innocuous.

The light in the library is fading. Yes, Mrs. Bok concludes, there are technologies whose intrusive potential bears watching. Yet much information is still our own.

"Sometimes people, I think, assume in this country that there is little that is private anymore, little that is secret," she says. "There I just think they are wrong, actually."

[From the Washington Post, Apr. 25, 1984]

GOVERNMENT TO SHARE DEADBEAT LIST WITH PRIVATE CREDIT-RATING BUREAUS

(By Pete Earley)

The Office of Management and Budget is putting the finishing touches on a debt collection system that will let federal agencies, for the first time, turn over to private credit bureaus the names of individuals and companies that owe the government money.

OMB officials aren't sure how many Americans have unpaid debts to federal agencies, but they believe that many of the deadbeats will be eager to pay once they learn that their credit rating could be affected.

At stake is an estimated \$18 billion in outstanding debts, 80 percent of it in unpaid loans owed to the Small Business Administration and the Departments of Agriculture, Education and Housing and Urban Development. Individuals who received overpayments from various federal entitlement and assistance programs owe an additional \$3 billion.

The OMB project also will give about 100 federal agencies direct computer access to credit bureau records, where financial information about more than 100 million individuals and companies is stored.

According to Joseph R. Wright, deputy OMB director, agencies will use the information to identify individuals and companies that have poor credit histories and to track persons who borrow from more than one agency. In the past, some borrowers have obtained new federal loans at the same time they were in default on a loan granted by a different agency.

Although the government has had access to credit records for several years, the new system will let agencies tap the records almost instantly, 24 hours a day, the OMB said.

The credit program is the culmination of three years of effort by the Reagan administration, which first had to persuade Congress to amend federal privacy laws to let the government and the private sector share financial information.

OMB expects the General Services Administration to finish negotiating contracts with seven national credit-reporting firms within a few months so that the information exchange can begin in October. Five of the credit firms collect computerized information about individuals. The other two collect credit data about companies.

When Wright first mentioned the project several months ago at a news briefing, he described it as a major example of how the administration will improve the government's debt collection process by using techniques that have been used successfully by private industry for years.

But OMB officials recently have been reluctant to discuss the project, saying any publicity would be premature.

"This is just not something that we want to talk about right now," an OMB spokesman explained last week.

This low-key approach is an abrupt shift for OMB, which has used such gimmicks as a five-foot-long check and trash bags filled with hundreds of federal reports to dramatize its campaign against federal fraud, waste and abuse.

Sources in the agency said the shift occurred, in part, because some administration officials are worried that the project might be "misunderstood" and many Americans "might become unduly worried" at the idea of federal agencies gaining access to large amounts of sensitive financial data.

Most credit bureau records include information about a person's income and the current status of bank loans, liens and credit card accounts. Some also include information about divorce records.

Marvin B. Kaplan, a spokesman for the Associated Credit Bureaus Inc., a trade association, said the federal Fair Credit Reporting Act of 1968 prevents such information from being misused.

That law would prohibit the government from reviewing an individual's credit record unless that person was under consideration for a federal loan, contract or job, Kaplan said. Law enforcement agencies can examine credit records for other reasons, but they must obtain a court warrant to review anything from the files other than names, addresses, former addresses and places of employment, Kaplan said.

In addition, anyone denied credit because of a credit bureau report also has a right to review the record and challenge it, Kaplan said.

COMPUTER MATCHING IS A SERIOUS THREAT TO INDIVIDUAL RIGHTS

JOHN SHATTUCK

More and more frequently, government agencies have been employing a new investigative technique: the matching of unrelated computerized files of individuals to identify suspected law violators. This technique—*computer matching*—provides a revolutionary method of conducting investigations of fraud, abuse, and waste of government funds. It permits the government to screen the records of whole categories of people, such as federal employees, to determine who among them also falls into separate, supposedly incompatible categories, such as welfare recipients.

Computer matching raises profound issues concerning individual privacy, due process of law, and the presumption of innocence. It also poses serious questions about cost effectiveness and the internal management of government programs.

COMPUTER MATCHING VERSUS INDIVIDUAL RIGHTS

To understand the impact of computer matching on individual rights, it is first necessary to grasp the difference between a computer-matching investigation and a traditional law enforcement investigation.

A traditional investigation is triggered by some evidence that a person is engaged in wrongdoing. This is true for cases of tax evasion, welfare fraud, bank robbery, or traffic speeding. The limited resources of law enforcement usually make it impracticable to conduct dragnet investigations. More importantly, our constitutional system bars the government from investigating

persons it does not suspect of wrongdoing.

A computer match is not bound by these limitations. It is directed not at an individual, but at an entire category of persons. A computer match is initiated not because any person is suspected of misconduct, but because his or her category is of interest to the government. What makes computer matching fundamentally different from a traditional investigation is that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin. That evidence is produced by "matching" two sets of personal records compiled for unrelated purposes.

There are four ways in which a computer match differs from a conventional law enforcement investigation in its impact on individual rights:

(1) Fourth Amendment

The Fourth Amendment protects against unreasonable searches and seizures, the most blatant of which have been "fishing expeditions" directed against large numbers of people. From the "writs of assistance" used in the eighteenth century by royal revenue agents, to door-to-door searches for violations of the British tariff laws in the American Colonies, to the municipal code inspections of the twentieth century to enforce health and safety standards, the principle that generalized fishing expeditions violate the right to be free from unreasonable searches has held firm in American law.

That principle is violated by computer matching. The technique of matching unrelated computer tapes is designed as a general search. It is not based on any preex-

listing evidence to direct suspicion of wrongdoing to any particular person. Although systematic searches of personal records are not as intrusive as door-to-door searches, the result is the same: a massive dragnet into the private affairs of many people.

(2) Presumption of Innocence

People in our society are not forced to bear a continuous burden of demonstrating to the government that they are innocent of wrongdoing. Although citizens are obliged to obey the law—and violate it at their peril—presumption of innocence is intended to protect people against having to prove that they are free from guilt whenever the government investigates them.

Computer matching can turn the presumption of innocence into a presumption of guilt. For instance, Massachusetts welfare recipients have been summarily removed from welfare rolls as the result of a computer match. These people fought for reinstatement based on information the state neglected to consider after their names appeared as "hits" in the match.

Another example of this "presumption of guilt" occurred three years ago in Florida. The state's attorney for a three-county area around Jacksonville obtained case files for all food stamp recipients in the area. He then launched fraud investigations against those receiving allotments of more than \$125 a month. A federal court of appeals invalidated the file search and enjoined the investigation on the ground that the targeted food stamp recipients were put in the position of having to prove the allotment they had received was not based on fraud. Construing the Food Stamp Act, the Court held that "it did not allow the [state food stamp] agency to turn over files . . . for criminal investigation without regard to whether a particular household has engaged in questionable behavior."

Once a computer match has taken place, any person whose name appears as a "raw hit" is presumed to be guilty. In part, this is because the technology of computer matching is so compelling and in part because its purpose—the detection of fraud and waste—is so commendable. The worst abuses of computer matching, such as summary termination of welfare benefits, have occurred when authorities have casually transformed this "presumption" into a conclusive proof of guilt.

(3) Privacy Act

The most important principle governing collection and use of personal information by the government is that

the individual has a right to control information about himself and to prevent its use without his consent for purposes wholly unrelated to those for which it was collected. This principle is imperfectly embodied in the Privacy Act of 1974.

The Privacy Act restricts disclosure by federal agencies of personally identifiable information—unless the subject consents. There are two major exceptions. The first involves a "routine use," defined as "the use of (a) record for a purpose which is compatible with the purpose for which it was collected." The second involves a "law enforcement" disclosure, which enables an agency to be responsive to a request by another agency for information relevant to the investigation of a specific violation of law.

When computer matching was in its infancy, the Privacy Act was correctly perceived by several federal agencies to be a major stumbling block. The Civil Service Commission initially balked in 1977 at the plans of Health, Education and Welfare (HEW) Secretary Joseph Califano to institute a match of federal employee records and state welfare rolls, on the ground that the use of employee records for such a purpose would violate the Privacy Act. The Commission's General Counsel, Carl F. Goodman, stated that the proposed match could not be considered a "routine use" of employee records, since the Commission's "information on employees was not collected with a view toward detecting welfare abuses." Similarly, it could not be considered a "law enforcement" use, continued Goodman, since "at the 'matching' stage there is no indication whatsoever that a violation or potential violation of law has occurred."

This reasonable interpretation of the Privacy Act soon gave way to a succession of strained readings. Since enforcement of the Privacy Act is left entirely to the agencies it regulates, it is hardly surprising that the agencies have bent the Act to their own purposes. They have now miraculously established that computer matching is a "routine use" of personal records. All that is required, they say, is to publish each new computer matching "routine use" in the *Federal Register*.

The Privacy Act has now been so thoroughly circumvented by executive action that it can no longer be seen as an effective safeguard. Nevertheless, the principle underlying the Act—that individuals should be able to exercise control over information about themselves that they provide to the government—is a bedrock principle of individual privacy. That principle is at war with the practice of computer matching.

A traditional investigation is triggered by some evidence that a person has engaged in wrongdoing. What makes computer matching fundamentally different is that its very purpose is to generate the evidence of wrongdoing required before an investigation can begin.

Under the Privacy Act of 1974, the individual has a right to control information about himself and to prevent its use without his consent for purposes wholly unrelated to those for which it was collected. That principle is at war with the practice of computer matching.

(4) Due Process of Law

Once a computer match has taken place, it will result in a series of hits. All those identified are in jeopardy of being found guilty of wrongdoing. To the extent that they are not given notice of their situation and an adequate opportunity to contest the results of the match, they are denied due process of law.

This is precisely what has happened in several matching programs. For example, the results of Secretary Califano's Operation Match were kept secret from federal employees whose records were matched with welfare rolls, because the Justice Department viewed the investigation "as a law enforcement program designed to detect suspected violations of various criminal statutes." The Justice Department ordered the Civil Service Commission not to notify any of the federal employees whose names showed up as hits, since "[t]he premature discussion of a specific criminal matter with a tentative defendant is in our view inimical to the building of a solid prosecutorial case." In Massachusetts, welfare authorities have terminated benefits of persons showing up as hits without even conducting an internal investigation.

This approach makes a mockery of due process. Due process is the right to confront one's accuser and introduce evidence to show that the accuser is wrong. When the accuser is a computer tape, the possibility of error is substantial. Keeping the subject of a raw hit in the dark increases the likelihood of an error's going undetected.

SOME COMMENTS ON THE OFFICE OF MANAGEMENT AND BUDGET'S (OMB'S) GUIDELINES

Since 1979 computer matching at the federal level has been regulated by guidelines issued by the OMB. These guidelines, which were considerably looser in May 1982, are intended to "help agencies relate the procedural requirements of the Privacy Act to the operational requirements of computerized matching." Although Kusserow cites the guidelines as evidence of the federal government's concern about privacy protection, in fact, they constitute an effort to paper over the profound conflict between (1) the Privacy Act principle that personal records are to be used by federal agencies only for purposes compatible with those for which they were compiled and (2) the computer matching practice

of joining personal records compiled for wholly unrelated purposes.

OMB's matching guidelines have rendered meaningless the central principle of the Privacy Act. In 1980, for instance, the Office of Personnel Management (OPM) published a notice in the *Federal Register* concerning its proposed use of personnel records for a matching program to help the Veterans' Administration (VA) verify the credentials of its hospital employees. The notice dutifully stated that the proposed match of OPM and VA records was a "routine use," which it explained as follows:

"An integral part of the reason that these records are maintained is to protect the legitimate interests of the government and, therefore, such a disclosure is compatible with the purposes for maintaining these records."

Under that broad justification any disclosure or matching of personal records would be permissible, since all federal records are purportedly maintained for the "legitimate interests of the government."

The guidelines, on which Kusserow so heavily relies, contain no requirements or limitations on the conduct of computer matching in these critical areas:

- (1) **The nature of the record systems to be matched—**There are no personal records, no matter how sensitive (e.g., medical files, security clearance records, intelligence records), that are beyond the reach of computer matching for any investigative purpose.
- (2) **The procedures to be followed in determining the validity of hits—**No particular procedures are required to insure that the subjects of hits are afforded due process of law.
- (3) **The standards and procedures to be followed for securing OMB approval of a proposed match—**Since the first guidelines were promulgated in 1979, OMB has not disapproved a single computer match.
- (4) **The projected costs and benefits of a proposed match—**The 1982 guidelines have deleted all reference to cost-benefit analyses or reports on computer matches. It is entirely at an agency's discretion whether to undertake a proposed match or to report the costs and benefits of the match.

It is impossible not to conclude that computer matching at the federal level is a huge unregulated business.

the only clear effect of which to date has been the undermining of individual privacy.

SOME EXAMPLES OF COMPUTER MATCHING

In the seven years since the technique was first used, over 200 computer matches have been carried out. At the federal level there have been matches for a wide variety of investigative purposes, using a broad range of personal record systems of varying degrees of sensitivity.

These include matches of federal employee records maintained by the Civil Service Commission with files of persons receiving federal Aid to Families with Dependent Children, to investigate "fraud"; federal personnel records maintained by OPM with the files of VA hospital employees, to check "accreditation"; federal personnel records of Agriculture Department employees in Illinois with Illinois state files on licensed real estate brokers, to "ascertain potential conflicts of interest"; Internal Revenue Service (IRS) records of taxpayer addresses with lists of individuals born in 1963 supplied by the Selective Service System, to locate suspected violators of the draft registration law; and Labor Department files of persons entitled to receive Black Lung benefits with Health and Human Services (HHS) records of Medicare billings, to investigate double-billing medical fraud.

These matches are only a handful of the total conducted. Even with these, very little hard data are available, thanks to the extraordinarily weak oversight and reporting requirements of the OMB guidelines and to the lack of attention to this subject by Congress.

CONCLUSION

Computer matching is an attractive investigative technique. It appears to permit law enforcement officials to instantaneously root out all instances of a particular kind of wrongdoing in a particular segment of the population. It constitutes a general surveillance system that supposedly can detect and deter misconduct wherever it is used. It appeals to the view that "if you haven't done anything wrong, you don't have anything to worry about."

But there are heavy costs associated with computer matching, both in terms of individual rights and in terms of law enforcement expenditure. It is not at all clear that the benefits of the technique outweigh the costs.

The comparison of unrelated record systems is fraught with difficulty. Data on the computer tapes may be inaccurate or inaccurately recorded. It may present an incomplete picture. It is unlikely to be sufficient to "answer" difficult questions, such as whether a person is entitled to receive welfare or is engaged in a conflict of interest.

On the other hand, computer matching erodes individual rights: the Fourth Amendment right to be free from unreasonable search, the right to the presumption

of innocence, the right to due process of law, and the right to limit the government's use of personal information to the purposes for which it was collected.

Moreover, the rapid and unchecked growth of computer matching leads inexorably to the creation of a de facto National Data System in which personal data are widely and routinely shared at all levels of government and in the private sector.

RECOMMENDATIONS

As a general framework for safeguarding individual rights, I propose the following:

- (1) The Privacy Act should be amended to clarify that computer matches are not ipso facto "routine uses" of personal record systems.
- (2) No further federal computer matches should be permitted without express congressional authorization.
- (3) Congress should not authorize computer matches of sensitive personal records systems (the confidentiality of which is otherwise protected by statute) such as taxpayer records maintained by the IRS, census records maintained by the Census Bureau, or bank records maintained by federally insured banking institutions.
- (4) No computer match should be authorized unless and until an analysis has been made of its projected costs and projected savings in the recoupment of funds owed to the government. The match should not be authorized unless the public benefit will far outweigh the cost—and unless individual rights will be protected. The results and full costs of any match should be published.
- (5) Procedural due process protections for the persons whose records are to be matched should be specified by statute, including the right to counsel, the right to a full hearing, and the right to confidentiality of the results of a match.

The thrust of my comments has been to raise some basic questions about computer matching. I recommend a moratorium on all further matching so Congress and the public can study the results of all computer-matching programs conducted to date and assess the long-term consequences.

In closing, I second the view of Justice William O. Douglas, when he said, "I am not ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."

Author's Present Address: John Shattuck, American Civil Liberties Union, 600 Pennsylvania Avenue, S.E., Suite 301, Washington, D.C. 20001.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

[From the New York Times, Oct. 31, 1984]

IRS REJECTED IN HUNT FOR ESTIMATED INCOME LISTS

(By David Burnham)

WASHINGTON, Oct. 30.—The three companies that compile computerized lists of the estimated incomes of most American households have refused to give the Internal Revenue Service access to their lists so it can test use the information to track down tax evaders.

The companies, in separate interviews, said such Government use of their lists would be improper and would not work. An executive of one of the companies called the project "absolutely ridiculous."

Their refusal appears to represent a significant setback to the \$700,000 I.R.S. plan to find out if the commercially prepared marketing lists can help the Government reduce the increasing number of Americans who pay no taxes. At the least, the refusals will delay the project a few months.

The three companies are the Donnelley Marketing Service of Stamford, Conn., the R.L. Polk Company of Detroit and Metromail of Lincoln, Neb.

COMBINE PUBLIC DATA

Each uses somewhat different computerized techniques to prepare its list. But in general, all are based on combining information from such publicly available sources as the Census Bureau, telephone directories and motor vehicle registrations in a way that allows the companies to identify virtually all households and many roughly accurate guesses about their incomes, family size and other characteristics.

Although the Internal Revenue Service refused to discuss the status of its project, a detailed I.R.S. description of it indicates that the service planned to initiate the test in six cities on Feb. 15. The computerized records of taxpayers in Brooklyn, Cheyenne, Wyo., Cleveland, Indianapolis, Milwaukee and Reno were to be matched against a computerized list showing the estimated income of all those living there.

The agency's description estimated that the list could cost up to \$100,000. But because of the lack of cooperation by the companies, the project is already at least two months behind schedule.

"I have just about given up trying to get a list for the I.R.S.," said Brandt Turner, an official with Dunhill of Washington, a company that specializes in locating mailing lists for Government agencies. "The possibility of success is rather low now."

CONGRESSIONAL PANELS WORRIED

In addition to the companies' objections, concerns about the implications of the experiment have been expressed by a Senate committee and two House subcommittees.

Recently, Representative Glenn English, chairman of the Government Operations Subcommittee on Government Information, Justice and Agriculture and Representative Doug Barnard Jr., chairman of the Subcommittee on Commerce, Consumer and Monetary Affairs, wrote the revenue service asking that they be kept fully informed about the experiment. Both Congressmen are Democrats, Mr. English from Oklahoma and Mr. Barnard from Georgia.

"There is clearly a need to explore reasonable, cost-effective methods of increasing the collection of tax revenues due the government," they told Roscoe L. Egger Jr., the Commissioner of Internal Revenue.

"At the same time, however," the Congressmen continued, "Federal agency plans to increase the compilation and computerization of personal information raise legitimate concerns about loss of privacy. It is not always easy to balance the competing interests of privacy and efficiency. This is a gray area, and it is important to proceed with caution, deliberation and knowledge."

Meanwhile, the Oversight Subcommittee of the Senate Government Affairs Committee, whose chairman is Senator William Cohen, Republican of Maine, has begun a separate inquiry. It is an extension of a series of hearings into the Government's increasing use of computers to match various official and industry files.

PROJECT CALLED ILL CONCEIVED

The Donnelley Marketing Service, a division of Standard and Poor's, is one of the principal developers of the lists, which have been used by direct-mail advertisers to reach special markets.

"It is inappropriate for the I.R.S. to use the kind of lists we produce to identify errant taxpayers," said Richard Vincent, director of marketing for Donnelley Marketing. "This I.R.S. experiment is ill conceived because such lists are not accurate on an individual basis, but only in the aggregate. We will have nothing to do with this project."

Explaining the uses of the lists for advertisers, Mr. Vincent said: "If a company wants to send a mailer to all American families with incomes over \$40,000, we rent it a list for a one-time use. Depending somewhat on the group the company wants to target, we guarantee that 75 or 80 percent of these receiving the material will have the correct characteristics."

He acknowledged that providing the revenue service with a list "would have been detrimental to our business."

"If we had responded, it probably would have inhibited some of those organizations that provide us with information used in the preparation of the lists from cooperating with us in the future," he said.

DATA UNRELIABLE FOR INDIVIDUALS

Reg Troncone, the executive vice president of Metromail, said the experiment was "absolutely ridiculous."

"We're not interested in providing the Government with information that is highly unreliable on an individual basis and that might be used in an improper way," he said.

Jack Casey, a spokesman for the third company, R. L. Polk, made the same point: "Polk believes the information it collects is useful for marketing purposes, but not for what the I.R.S. is considering here. We're not going to sell to the Government."

Mr. Turner of Dunhill, who has a contract to obtain a list for the revenue service, questions the motivation of the companies in refusing to make their lists available. "I happen to know that until The New York Times carried an article about the I.R.S. experiment several weeks ago, at least one of the big three was actively interested in a deal," he said. "This is not so much a matter of principle, it is a question they don't like this kind of publicity."

In the perspective on the project, the Federal agency said it was already using third-party reports such as wage statements and truck registrations to develop leads on what it calls nonfilers.

"There are some sources of income, however, for which information returns are not required to be filed or for which information return filing compliance is poor," the agency said. "Thus, there are gaps in the service's ability to identify individual nonfilers."

"To help close the gap," it said it should test commercial lists containing "an estimate of household income, based on an analysis of personal consumption indices such as automobile ownership, real estate transactions and published census data."

Under the original schedule, which the I.R.S. now will probably not meet, the Government planned to match the computerized lists of all taxpayers in the six test districts against the commercially produced list of households. Evaluation of whether the technique was effective was to be completed on May 31, 1985.

Although the agency could prepare its own lists by using the same information sources as the companies, experts believe this is unlikely because it would be so expensive. Private companies can afford to prepare the lists because the cost is shared by the many marketing companies that rent them.

Report from the Center for



**PHILOSOPHY &
PUBLIC
POLICY**

University of Maryland • College Park, Maryland 20742 • Telephone: 301-454-4103

Volume 4, Number 3
Fall 1984

Privacy in the Computer Age

To make its research readily available to a broad audience, the Center for Philosophy and Public Policy publishes a quarterly newsletter, *QQ—Report from the Center for Philosophy and Public Policy*. Named after the abbreviation for "questions," *QQ* summarizes and synthesizes Center books and working papers and features other related work on public policy questions. Articles in *QQ* are intended to advance philosophically informed debates on current policy choices; the views presented are not necessarily those of the Center or its sponsors.

In this issue:

New computer technology has led to the growth of enormous centralized databases storing vast quantities of personal information about all of us. Does this pose a threat to privacy, and if so, what kind of a threat? What is privacy and why do we value it personally and as a society? p. 1

A committed feminist perspective is not only compatible with the traditional teaching of philosophy and public policy, but may be one of its central requirements. p. 6

The emergency opens the factory, but a whole community can be questioned if it shuts down. Who should have the right to make a decision that affects so many people so deeply? p. 9

A member of the recent presidential commission on biomedical research explores the painful and perplexing moral issues raised by the case of Baby Jane Doe. p. 12

The Security Council's Deterrence Dilemma in the Nuclear Age is presented. p. 15

The odds are good that some computer somewhere knows something about you that you would rather it didn't. The databases of the federal government contain 4 billion separate records about American citizens — seventeen items apiece. Recently, different government files have been electronically compared to uncover tell-tale discrepancies: personnel files of federal employees have been matched against state welfare rolls to flag welfare fraud; lists of eighteen-year-old male dependents generated from IRS records have been matched against Selective Service registrations to identify draft evaders. The FBI's National Crime Information Center is a massive computer network linking more than 57,000 federal, state, and local criminal justice agencies and offering instant access to information on stolen property, missing and wanted persons, and criminal histories. This last category is of particular interest to prospective employers, who were responsible for half of the over 200 million inquiries directed to the network last year. It's worth their while to bother checking; one in five Americans will be arrested at some time in their lives.

The federal government is joined in its computerized information gathering by behemoths in the private sector. A giant computerized credit company like TRW makes available to thousands of merchants all over the country a tidy balance sheet on any of almost 90 million Americans in a matter of three or four seconds. AT&T holds precise minute-by-minute records of the 500 million phone calls made daily from the nation's 130 million telephones, information that has been used by government investigators

Report from the Center for
 Philosophy
 and Public Policy

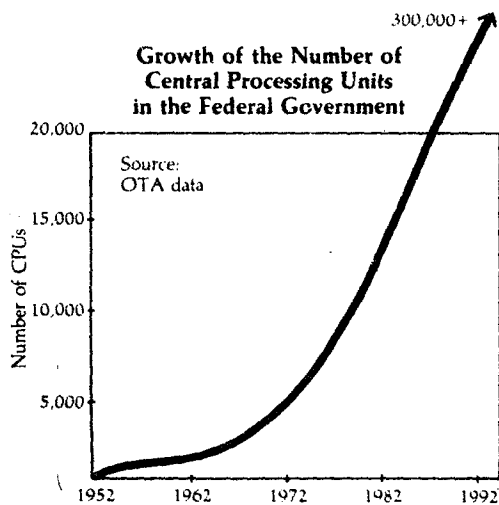
in a number of cases. Such information, notes David Burnham, author of *The Rise of the Computer State*, "can be extraordinarily revealing. . . investigators can learn what numbers an individual has called, what time of day and day of week the calls were made, the length of each conversation, and the number of times an incorrect number was dialed. Considered as a whole, such information can pinpoint the location of an individual at a particular moment, indicate his daily patterns of work and sleep, and even suggest his state of mind."

In many businesses, computers are used directly and overtly for worker surveillance. A recent nationwide survey of video display terminal operators showed that 35 percent were monitored by computer. Computer monitoring has been used to keep a daily log of the room-tidying speed of maids at Washington's Ritz-Carlton Hotel, to clock the "average work time" of AT&T telephone operators, to see how fast the cashiers at the Giant Food Store process customers, and to tabulate the performance of United Parcel drivers to the hundredth of an hour.

Many charge that these cases amount to a flagrant and frightening invasion of privacy. They ask whether privacy in any recognizable form can survive the computer age. But just what kind of a threat to privacy is posed by the long memory and unblinking eye of the computer? What is privacy and why do we value it personally and as a society? How do we weigh the threatened value of privacy against the manifold marvels the computer promises to unfold before us?

What Is Privacy?

Privacy has been defined in a number of ways. On one account, it is the measure of *control* a person has over access



to information about herself, or to the most intimate aspects of her life. Privacy is a matter here, not of how much others know about the details of one's life, but of the extent to which the person herself decides what information they are to have. On another account, privacy is the *state* or *condition* of limited access to a person. On this view, someone's privacy is diminished in some measure whenever others come to know more about her.

Ferdinand Schoeman, a professor of philosophy at the University of South Carolina currently in residence at the Center for Philosophy and Public Policy, favors the second account. He argues that "a person who chose to exercise his discretionary control over information about himself by divulging everything cannot be said to have

There are important gains that come from living in a society in which certain kinds of derogatory information about an individual are permitted to disappear from view after a certain amount of time. What is involved is the creation of a kind of social environment that holds out . . . the possibility . . . of genuine individual redemption.

lost control, although he surely cannot be said to have any privacy." And an individual can lose some control over access to personal information (if, for instance, a national security agency is authorized to monitor international phone conversations) without losing any privacy at all (if his conversations are not among those monitored). The right to privacy, according to Schoeman, has to do with the question of the individual's control; privacy itself concerns what the individual has control of.

Thus either privacy itself or certainly the right to privacy is diminished when huge databases stock vast quantities of information about us (and particularly when computerized matching programs reveal to one agency, without our authorization, information disclosed to another). Access to personal information about us is increased, and our control over who has access to this information, and what kind of access, is decreased.

Why does this matter? Why is it important that access to information about our lives remain limited, or that we control such access?

Why Privacy Matters

One reason why we might value privacy is that it carves out a space within which we can do bad things without being found out. Those with criminal intentions have good reason to ward off too-close scrutiny of their affairs. But this reason for valuing privacy will not carry much weight with the rest of us, who have nothing criminal to hide. We would rather eliminate welfare fraud than shield the defrauder from a computerized matching program that would uncover his double identity.

Privacy also allows the convicted miscreant the hope that in time her past misdeeds will fade from public attention and be forgotten. The FBI's master file of computerized histories ensures, on the contrary, that memory will be steadfast and long. Legal theorist and now federal judge Richard Posner argues that this is all to the good, that people should be thwarted in concealing disadvantageous information about themselves. Such concealment, he thinks, amounts to fraud in "selling" oneself to prospective employers and friends. But Richard Wasserstrom, professor of philosophy at the University of California at Santa Cruz, suggests that "there are important gains that come from living in a society in which certain kinds of derogatory information about an individual are permitted to disappear from view after a certain amount of time. What is involved is the creation of a kind of social environment that holds out to the members of the society the possibility of self-renewal and change . . . of genuine individual redemption."

Those who would have nothing to fear from the disclosure of complete and accurate information about themselves might, of course, have a good deal to fear from the disclosure of partial and false information. Unfortunately partial and false information are just what most databases have an abundance of. Burnham reports the results of one study that found that only 45.9 percent of the records in the FBI's computerized criminal history file were "complete, accurate, and unambiguous." Anyone who has tangled with a computer over a simple billing error knows how difficult it can be to erase a faulty bit of information from the computer's elephantine memory. Furthermore, even accurate information can be subject to misinterpretation; Burnham also points to sociological experiments indicating that employers are reluctant to hire workers with arrest records, even where charges were later dropped, or where a court trial resulted in acquittal. Once arrested, one is presumed guilty even after being proved innocent! While privacy per se is not at issue in the disclosure of *false* information about ourselves, it at least reduces the sheer volume of personal information stored, thus minimizing the danger of error.

By enhancing and fostering a clear sphere of the private, privacy helps to rein in the sphere of the public, to mark out a clear boundary that we prohibit the state from crossing.

People differ in how approvingly they regard the current government, but no one has much trouble imagining some possible future government that would be far worse. It seems wise, then, to curb the power of the state over its citizens, to make sure that the state doesn't come to know too much. By enhancing and fostering a clear sphere of the private, privacy helps to rein in the sphere of the public, to mark out a clear boundary that we prohibit the state from crossing. It is the crossing of this boundary that is feared



Photo courtesy of International Business Machines Corporation

The FBI's National Crime Information Center offers instant access to information on stolen property, missing and wanted persons, and criminal histories.

when computerized databanks are likened to an Orwellian Big Brother.

These concerns, however potent, still do not seem to capture all there is that matters to us about preserving our privacy from computerized intrusions. If these doubts could be met in other ways — by strictly enforcing a periodical review of stored records for completeness and accuracy, say, or erecting other barriers against official abuse — we would still feel that there was some deeper worry left untouched. Privacy is important not only for what it saves us from, but for what it has been argued to make possible: freedom and dignity, on the one hand, and intimate human relationships, on the other.

Freedom and Dignity

Privacy protects freedom: not only the freedom, as noted earlier, to misbehave, but the freedom to do anything that we would be inhibited in doing by the presence of external observation. Think how many actions we would feel less free to perform if there were someone — anyone — intently watching us every minute of the day, taking account of every movement we made, every syllable we uttered. Such relentless scrutiny would make one reluctant to do anything commonly perceived, for whatever reason, as foolish or embarrassing; it would curtail groping, experimentation, risk taking, trial and error. Imagine trying to write a paper, a poem, a love letter, with every preliminary scribble inspected by an uninvited third party. We are less free to act, to speak, to dream in public:



than in private, and practices of privacy maintain the barrier between the two realms.

Do current uses of computer technology undermine privacy in a way that poses a threat to freedom? The minute-by-minute computerized surveillance of workers that is increasingly relied upon as a management technique seems clearly to make workers less free. When, as in some workplaces, every keystroke is tallied electronically, every momentary respite recorded — every nose-blowing, every stretch, every bathroom break — the state of observation is too total, and too totalitarian.

Privacy is a social ritual by means of which an individual's moral title to his existence is conferred. Privacy is an essential part of the complex social practice by means of which the social group recognizes — and communicates to the individual — that his existence is his own.

To a much lesser degree, projected levels of centralized data collection and storage could also take a toll on freedom and spontaneity. With the routine storage of enormous quantities of information, Wasserstrom speculates, "every transaction in which one engages would . . . take on an additional significance. In such a society one would be both buying, a tank of gas and leaving a part of a systematic record of where one was on that particular date. . . . An inevitable consequence of such a practice of data collection is that persons would think more carefully before they did things that would become part of the record. . . . we would go through life encumbered by a wariness and deliberateness that would make it less easy to live what we take to be the life of a free person."

Privacy is critical as well to the affirmation of human dignity. Jeffrey Reiman, a philosopher at American University, suggests that the cluster of behaviors that makes up the social practice of privacy has as its purpose a resonant societal declaration of respect for the dignity of the individual: "Privacy is a social ritual by means of which an individual's moral title to his existence is conferred. Privacy is an essential part of the complex social practice by means of which the social group recognizes — and communicates to the individual — that his existence is his own."

The right to privacy, on Reiman's view, "is the right to the existence of a social practice which makes it possible for me to think of this existence as *mine*." The specific nature and form of this practice may differ from society to society and may change over time. This means that the growth of computerized databanks need not undermine privacy in our society if other practices in the complex privacy ritual receive compensatory emphasis or new practices develop. But there is a danger that the weakening of one strand in the cluster will weaken others as well. Wasserstrom warns, "If it became routine to record and have readily accessible vast quantities of information

about every individual, we might come to hold the belief that the detailed inspection of any individual's behavior is a perfectly appropriate societal undertaking. We might become insensitive to the legitimate claims of an individual to a sphere of life in which the individual is at present autonomous and around which he or she can erect whatever shield is wished."

Privacy and Intimate Relationships

In one sense, privacy builds fences around persons through which others are not permitted to peer and beyond which they may not trespass. The right to privacy has been categorized as the right to be let alone. Yet here, too, it has been argued that "good fences make good neighbors" — that privacy not only protects individual freedom and dignity but is itself a necessary precondition of our entering into a wide range of diverse human relationships.

According to University of Alabama philosopher James Rachels, "There is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people." An essential part of what distinguishes one sort of relationship from another is "a conception of the kind and degree of knowledge concerning one another which it is appropriate for [the parties] to have." Thus we disclose different amounts of information about different aspects of our lives to our doctor, employer, neighbors, children, casual acquaintances, close friends, spouse. If we could not control the level of disclosure and choose to be selective in our revelations, Rachels argues, we could not maintain an array of diverse personal and professional relationships.

Indeed, Charles Fried insists that without privacy our most intimate relationships "are simply inconceivable. To be friends or lovers persons must be intimate to some

Intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.

degree with each other. But intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love. . . . Privacy grants the control over information which enables us to maintain degrees of intimacy.

Is the possibility of genuine sharing within an intimate relationship precluded by the proliferation of centralized databanks in which the secrets that would be confided to the loved one are handily stored with billions of other tid-



University of Maryland Computer Science Center



The very impersonality of the computer's storage of intimate information can give rise to a feeling of violation.

bits of information on a magnetic tape? The answer would seem to depend in part on how many people in what capacity have access to the database. The Rachels-Fried view provides one argument for limiting access as far as possible — for not, for example, passing files about from one government agency to another.

Reiman argues, however, that Fried and Rachels are wrong to think that intimacy is bound up with privacy in the way they propose. Their view, he feels, "suggests a market conception of personal intimacy. The value and substance of intimacy — like the value and substance of my income — lies not merely in what I have but essentially in what other do *not* have." Intimacy, on this view, is constituted by its unavailability to others — in economic terms, by its scarcity. Reiman suggests instead that "what constitutes intimacy is not merely the sharing of otherwise withheld information, but the context of caring which makes the sharing of personal information significant." He goes on to say, "It is of little importance who has access to personal information about me. What matters is who cares about it and to whom I care to reveal it. Even if all those to whom I am indifferent and who return the compliment were to know the intimate details of my personal history, my capacity to enter into an intimate relationship would remain unhindered." Computers are no threat to intimacy on this view. What matters for intimacy is not how much some computer knows, but how much some human being cares.

Computers don't care, of course, and likely the human beings who input intimate information into a database at so many keystrokes a minute don't care, either. This in itself can give rise to a feeling of violation — Schoeman observes that we feel defiled when information that matters deeply to ourselves is handled without recognition of its specialness. He compares intimate information, information that is of the greatest importance to our conception of ourselves, to a holy object — "something that is appropriately revealed only in special circumstances. To use

such an object, even though it is a humble object when seen out of context, without the idea of its character in mind is to deprive the object of its sacredness. . . . Such an abuse is regarded as an affront."

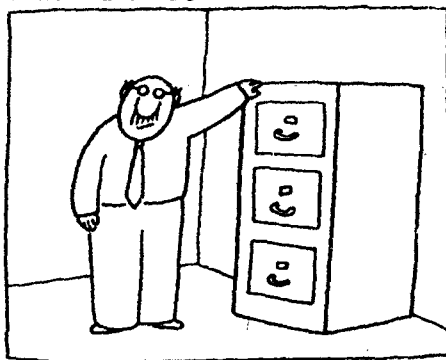
None of this is to say that records of intimate information should not be committed to the computer. There are in many cases weighty societal reasons for collecting and storing the information that we do. But it is a good thing for us to remember periodically that the data we collect and analyze and scrutinize are at bottom a record of people's lives. We have a charge to treat them carefully, and with respect.

Conclusion

It is common to assume that technological changes inevitably pose a threat to privacy. But Schoeman notes that the industrial revolution brought in its wake a major increase in privacy, as the resultant urbanization led to heightened anonymity — "the privacy that results from the indifference of others." Generally, Schoeman suggests, "the degree to which privacy is threatened is a function of design rather than of mere consequence." The technology of the computer gives us new capabilities that would allow us to restrict the privacy of individuals in new ways, but it does not dictate how we will choose to use them. That choice depends on how important we, as a society, take privacy to be.

The views of Ferdinand Schoeman, Richard Posner, Richard Wasserstrom, Jeffrey Reiman, James Rachels, and Charles Fried are taken from their article in Philosophical Dimensions of Privacy: An Anthology, edited by Ferdinand Schoeman (Greenwich, Connecticut: University Press, 1984). The factual information in this article is drawn from The Rise of the Computer State, by David Burdick (New York: Young Books, 1984) and two articles that appeared in the Washington Post: "The Computer That Can Read Your Mind," by Bob Brown, September 23, 1984; and "Violating the Computer State's Envelope Concern," by Peter Fox, September 2, 1984.

PRIVATE FILES



Drawing by C. Barsotti © 1984
The New Yorker Magazine, Inc.

Law

The No Man's Land of High Tech

New devices aid police but threaten the right of privacy

On the morning of Nov. 2, 1983, Francis Lynch, then chief of detectives of the Woonsocket, R.I., police department, got a strange call. "You may think I'm crazy," said an excited young woman, "but there is some guy dealing drugs, and I can hear it on my radio." Lynch was skeptical, but he sent two detectives to the woman's house.

It turned out that the transmissions that the woman had heard on her AM radio were coming from a nearby home whose occupant, Leo DeLaurier, owned a cordless telephone. DeLaurier was apparently unaware that such devices are little more than short-range radio transmitters whose signals can sometimes be picked up by ordinary radio receivers. During the next month, the police say, they recorded more than 100 hours of incriminating conversations by DeLaurier about the sale of cocaine and marijuana. Then they arrested DeLaurier, his wife and 22 other people on drug charges. DeLaurier objected to the use of the tapes, and his trial has been postponed pending the outcome of an appeal to the Rhode Island Supreme Court. DeLaurier argues that the monitoring of his phone was an illegal invasion of his privacy since it was done by the police without a warrant.

Legal experts point out that cordless phones are one of many new-age technological devices that fall into a legal no man's land, an ambiguous region inhabited by such consumer products as personal computers and the ubiquitous message beepers and by sophisticated police equipment like mini-video cameras. The lack of clear legal rules for police use of the equipment promises to keep the courts busy. Just last month two federal courts clashed on the issue when the U.S. Court of Appeals for the Seventh Circuit in Chicago overruled a federal district court and found that video surveillance of four suspected members of the Puerto Rican terrorist group FALN did not violate the Fourth Amendment's guarantee against "unreasonable searches and seizures." Says University of Chicago Law Professor Geoffrey Stone: "Technology—bugs, beepers that police attach to cars, parabolic microphones—all of this enables the Government to invade privacy in ways far more extreme than one could possibly have imagined when the Fourth Amendment was written."

The Kansas Supreme Court was the first state high court to rule on the cordless-phone issue, holding last March that those who use such phones are broadcast-

ing over the public air waves and have "no reasonable expectation of privacy," a finding that may surprise the 7 million or so owners of the popular instruments. But to rule otherwise, Rhode Island's attorneys argued before that state's supreme court, could mean that the woman who inadvertently overheard DeLaurier's conversations might be held criminally liable for violating the federal wiretapping law.



DeLaurier's lawyer, however, asserted that this 1968 legislation, which forbids wiretapping without court authorization, does apply to cordless phones, since the statute defines a "wire communication" as any conversation that is carried "in whole or in part" by wire. Even cordless instruments must utilize regular phone lines at some point to transmit calls.

Video surveillance is as knotty an issue as the new telephones. Abscam, the DeLoe drug investigation and other well-publicized "sting" operations have made it seem that police have broad authority to videotape criminal activity. In fact, cameras have usually been employed to record only those meetings where an undercover agent or informer with prior knowledge of the filming is also in the room. This was not the situation in the Chicago FALN case, in which the FBI had authorization for both audio and video surveillance from a federal judge. The agency resorted to the video surveillance of two "safe house" apartments after two of the four suspects successfully thwarted wiretaps and bugs

Once the cameras had been installed, agents say, they observed some of the defendants constructing time bombs. The four were arrested in June 1983 on seditious-conspiracy and weapons charges when the FBI learned that they allegedly planned to mark the July 4 holiday by blowing up military installations.

U.S. District Judge George Leighton threw out the FBI's 130 hours of videotape evidence in 1984, saying that "no one, not even in the name of ferreting out crime, has the right to invade the privacy of a home" without proper legal authority. He ruled that the 1968 wiretap law provided no such authority because it says nothing about video surveillance. The Seventh Circuit panel, in an opinion written by Supreme Court hopeful Richard Posner, held that the wiretap law did not apply but found that video surveillance is permitted under the Constitution without specific legislative approval. Paraphrasing a famous dissent by Justice Louis Brandeis, Posner wrote, "There is no right to be let alone while assembling bombs in safe houses." The accused FALN members plan to appeal the ruling to the U.S. Supreme Court.

Many legal observers are frightened by the prospect of widespread video surveillance. Raising the specter of *Nineteen Eighty-Four* and Big Brother, Herman Schwartz, a law professor at American University, denounces it as "very dangerous" to everyone's civil liberties. Harvard Law Professor Laurence Tribe cautions that technological innovations like video cameras may be rendering the traditional protections of the Fourth Amendment "irrelevant." Columbia University Law Professor Richard Uviller, a former proctor, says of the new high-tech snooping: "When there is no alternative, when the crime is terror, there is a strong law-enforcement need for this." But he adds that "its uses should be reserved for only the most serious circumstances: kidnaping, murder, espionage and terrorism."

To clarify the legal muddle, several federal statutes have been proposed, including one by Wisconsin Congressman Robert Kastenmeier that would force police to satisfy a series of strict requirements in order to get a warrant for video prying. Though the Kastenmeier bill died in the last Congress, it will be reintroduced in this session. Judges, legislators and civil libertarians agree that the privacy problems presented by technological changes make necessary a new assessment of existing statutes and court rules. Warns John Shattuck, a former American Civil Liberties Union official: "In many ways, technology is now outstripping the law." —By Michael S. Sorell

Reported by Carol Fletcher/Chicago and Timothy Loughran/New York

The Direct Mail
Marketing Association's
Suggested
Guidelines for

**Personal
Information
Protection**

dm
ma

The Direct Mail/Marketing Association's Personal Information Protection Guidelines are intended to provide individuals and organizations involved in direct mail and direct marketing with principles of conduct that are generally accepted. These Guidelines reflect DMMA's long-standing regard for personal privacy and the responsibility of direct marketers to the consumer—a relationship that must be based on fair and just principles.

These Guidelines are also a part of the DMMA's general philosophy that self-regulatory measures are more desirable than governmental mandates whenever possible. Self-regulatory actions are more readily adaptable to changing techniques, economic and social conditions, and they encourage widespread use of sound and responsible business practices.

Because it is believed that a concern for everyone's privacy with respect to truly personal information is a basis for good business practices within direct response marketing, observance of these Guidelines by all concerned is recommended.

The Direct Mail/Marketing Association recognizes the need for businesses to protect the personal privacy of individuals and their need to provide safeguards for the proper handling of personal data contained in data files. DMMA strongly believes that good business practices require respect for such expectations of the individual.

Accordingly, DMMA recommends the following Guidelines for the handling of personal data in data files.—

For purposes of these Guidelines, the following definitions apply:

Individual: A natural person identified in a file by name and address or other identifier.

Personal Data: Information which is linked to an individual on a file and which is not publicly available or observable.

Direct Marketing Purposes: The purposes of direct marketing are to promote, sell and deliver goods and services; to foster such efforts through the sale, rental, compilation or exchange of lists in accordance with the principles of these Guidelines; to delete and add individuals to lists; to provide all necessary customer services including the extension of credit where appropriate; to raise funds; to perform market research and to encourage recipients to respond by taking direct action.

Article 1. Personal data should be collected by fair and lawful means for a direct marketing purpose.

Article 2. Direct marketers should limit the collection of personal data to only those data which are deemed pertinent and necessary for a direct marketing purpose and should only be used accordingly.

Article 3. Personal data which are used for direct marketing purposes should be accurate, complete and should be kept up to date to the extent practicable by the direct marketer. Personal data should be retained no longer than is required for the purpose for which they are stored.

Article 4. An individual shall have the right to request whether personal data about him/her appear on a direct marketer's file and to receive a summary of the information within a reasonable time after the request is made. An individual has the right to challenge the accuracy of personal data relating to him/her. Personal data which are shown to be incorrect should be corrected.

Article 5. Personal data should be transferred between direct marketers only for direct marketing purposes. Every list owner who sells, exchanges or rents lists containing personal data should see to it that each individual on the list is informed of those practices (Self Disclosure), and should offer an option to have the individual's name deleted. The list owner should remove names from his/her lists when requested directly in a signed writing by the individual, or by use of the DMMA Mail Preference Service name removal list.

List brokers and compilers should take reasonable steps to have the list owner follow these list practices.

Personal data should not be put at the disposal of any third party except as set forth in these Guidelines, or with the express consent of the individual, unless required by law.

Article 6. All list owners, brokers and compilers should be protective of the individual's right to privacy and sensitive to the information collected on lists and subsequently considered for transfer.

Personal information supplied by individuals such as, but not limited to, medical, financial, insurance or court data

should not be included on lists that are rented or exchanged when there is a reasonable expectation by the individual that the information would be kept confidential.

Article 7. Each direct marketer should be responsible for the security of personal data. Strict measures should be taken to assure against unauthorized access, alteration or dissemination of personal data. Employees who have access to personal data should agree in advance to use those data only in an authorized manner.

Article 8. Visitors to areas where personal data are processed and stored should be specifically authorized by express permission of the direct marketer and should be accompanied by at least one authorized employee of the direct marketer.

Article 9. If personal data are transferred from one direct market to another for a direct marketing purpose, measures should be taken by the transferor to arrange strict security measures to assure that unauthorized access to the data is not likely during transfer procedures. It is the responsibility of the direct marketer to whom the list is transferred to arrange strict security measures to insure no unauthorized access to the list during its return to the original owner.

Article 10. The Committee on Ethical Business Practices of DMMA is charged with reviewing any complaints by individuals of violation of these Guidelines and shall take appropriate action.

DMMA Ethics Department

In its continuing efforts to improve the image of direct mail and direct marketing, DMMA sponsors several activities in its Ethics Department.

Ethical Guidelines are maintained, updated periodically and distributed to the field.

A Committee on Ethical Business Practices monitors the mails and direct offerings to the consumer and investigates complaints brought to its attention.

An Ethics Policy Committee initiates programs and projects directed toward improved ethical activity in the direct marketing area.

MOAL (Mail Order Action Line) handles consumer mail order complaints and MPS (Mail Preference Service) offers mail flow reduction or increased specialized mail to consumers.

All Ethics activities are directed by a full time Director of Ethical Practices.

For additional information contact:

John M. Cavanaugh

Director, Ethical Practices

Direct Mail/Marketing Association, Inc.
6 East 43rd Street, New York, NY 10017
(212) 689-4977

•
Suite 905, 1730 K Street, N.W.
Washington, DC 20006
(202) 347-1222

Members of DMMA proudly display this symbol and slogan:

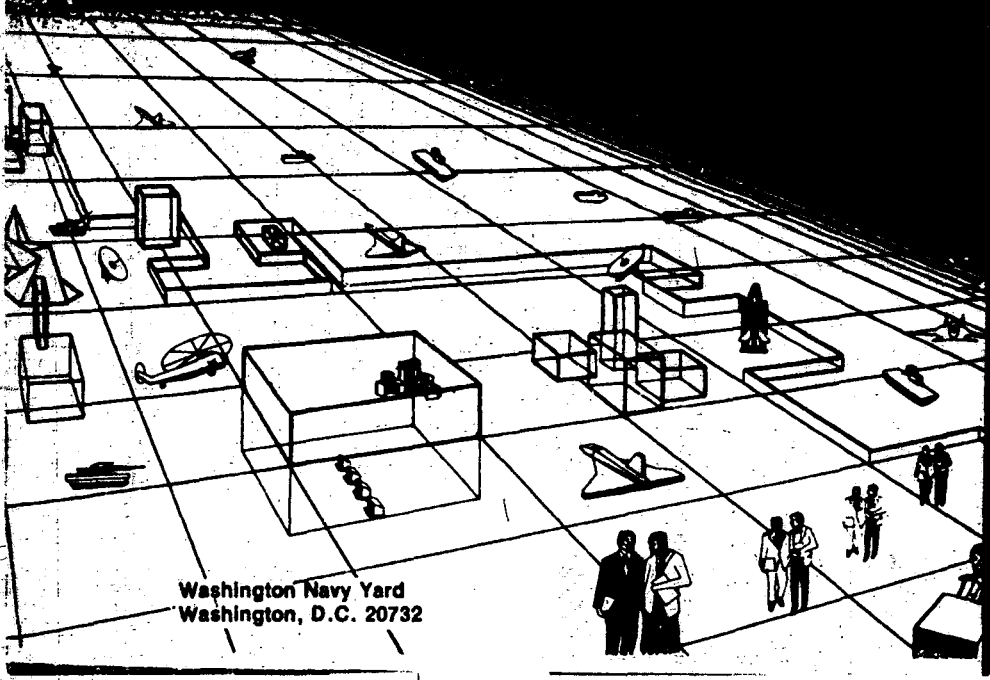


"Look for this symbol when you buy direct."

National Defense University
Department Of Defense Computer Institute



SELECTED COMPUTER ARTICLES 1983-84



Washington Navy Yard
Washington, D.C. 20732

CONTENTS

1 Information Resources Management

- 3 Information Resource Management in the 80's
Herbert R. Brinberg
Information and Records Management, March 1982
- 6 Records, Words, Data . . . Whatever You Call It,
It's Still Information, Part 1
Rita Mass
Information and Records Management, June 1982
- 9 Records, Words, Data . . . The State of Information
Management, Part 2
Rita Mass
Information and Records Management, July 1982
- 12 One Year Later: Reacting to the Act
Louise G. Becker
Government Data Systems, January/February 1982
- 15 Information Management — Czardom or Stardom?
Forest W. Horton
Information and Records Management, July 1981
- 17 Manager or Technician? The Nature of the
Information Systems Manager's Job
Blake Ives & Margrethe H. Olson
MIS Quarterly, December 1981
- 32 Decision Support Systems: An MIS Manager's
Perspective
Robert K. Vierck
MIS Quarterly, December 1981

2 Management Concerns

- 49 Coping with Computer Proliferation
Frederic G. Withingto
Harvard Business Review, May/June 1980
- 62 Anticipating the Forces of Change
Robert V. Head
Government Data Systems, May/June 1982
- 63 Information Systems and Organizational Change
Peter G. W. Keen
Communications of the ACM, January 1981
- 73 Life Cycle Management
Carl Hämmer
Information and Management, May 1981
- 83 Portfolio Approach to Information Systems
F. Warren McFarlan
Harvard Business Review, September/October 1981
- 92 Managing Information Systems by Committee
Richard L. Nolan
Harvard Business Review, July/August 1982
- 100 Reaching for Higher Productivity? First Get a
Grip on What It Is and How DP Will Measure It
Paul J. Meyer
Data Management, October 1980

- 103 Turning Around Turnover
Stanley R. Acker
Data Management, March 1981

3 Computer Security

- 109 Computer Crime: Insecurity in Numbers
Ivars Peterson
Science News, July 3, 1982
- 112 The Democratization of White Collar Crime
Robert H. Courtney
Computer Security Journal, Spring 1981
- 118 Breaching System Security
Robert Bernhard
IEEE Spectrum, June 1982
- 126 20 Questions on Computer Software Security
Al Iagnemma
Security World, September 1981
- 130 Software Security: Legal Aspects and Traditional
Considerations
Steve Geynes & Jerry M. Dehay
Journal of Systems Management, April 1981
- 135 An Auditor Looks at Computer Security
Richard Frescura
Security Industry and Product News, July 1981
- 138 Tactical Planning for Data Security Management
Sandra M. Mann
Data Security Management, 1982
- 148 Computer Security: A Current Assessment
Samantha Fordyce
Computers and Security, January 1982
- 156 Contingency Planning: An Opportunity for DP
Management
Terrence J. Boyer
Computer Security Journal, Winter 1982
- 165 Office Automation Systems: Problem Area of the 80's
William A. J. Bound
Security Industry and Product News, November 1981
- 167 Computers and the Future
Jagdish R. Dalal
Journal of Systems Management, August 1981

4 Privacy

- 175 Privacy Expectations in an Information Age
Jeffrey A. Meldman
Computer Security Journal, Winter 1982
- 184 Cable TV Could Be the Peeping Tom of the 80's
Fred Graham
TV Guide, July 1981

- 185 **Privacy: Still Threatened**
Robert E. Smith
Datamation, September 1982
- 190 **Privacy: A Naggig DP Problem**
Steve Stibbens
Infosystems, August 1982
- 193 **Security and Privacy in the 80's**
Willis Ware
Rand Paper P-6492, 1980
- 5 Systems Analysis and Design**
- 205 **Designing Corporate Information Systems**
Monika Kirtland
Information and Records Management, March 1982
- 208 **Modeling for MIS**
Brent Bowman; Gordon Davis; & James Wetherbe
Datamation, July 1981
- 213 **What Users Want**
John A. Moynihan
Datamation, April 1982
- 215 **How to Design with the User in Mind**
Ben Shneiderman
Datamation, April 1982
- 217 **Userware: The Merging of Systems Design and Human Needs**
Joel R. Lapointe
Data Management, February 1982
- 222 **Structured Programming**
Randall W. Jensen
Computer, March 1981
- 6 Computer Systems Acquisition**
- 239 **Getting Ourselves Together on Systems Acquisition**
Vincent Puntano
Defense/81, October 1981
- 250 **It Ain't Necessarily So**
Francis A. McDonough
Government Data Systems, July/August 1982
- 254 **New Directions in ADP Acquisition**
Donald W. Sawyer
Signal, July 1982
- 257 **Smart Benchmarking—The Key to Successful Procurement???**
John Seaman
Computer Decisions, March 1981
- 267 **Standard Benchmarks Aid in Competitive System Selection**
Robert V. Head & Norris S. Goff
Journal of Systems Management, January 1979
- 7 Software**
- 275 **A History of Operating Systems**
Norman Weizer
Datamation, January 1981
- 281 **The New Operating Systems: Sophistication, Compatibility and Power**
Paul G. Truax
Government Data Systems, March/April 1982
- 285 **A Human-Factors Style Guide for Program Design**
Henry Simpson
Byte, April 1982
- 294 **Plan Software Maintenance Now; Save Time and Dollars Later**
John B. Munson
Data Communications, June 1982
- 299 **EDP User Documentation: The Missing Link**
Susan J. Grimm
Journal of Systems Management, November 1980
- 305 **Ada: A Promising Beginning**
William E. Carlson
Computer, June 1981
- 8 Data Base**
- 311 **Relational Data Bases**
Myles E. Walsh
Journal of Systems Management, June 1980
- 316 **Relational Data Base: What Is It. What Can It Do?**
Ronald L. Dumas
Data Management, January 1981
- 319 **Evaluating Database Languages**
Jeffrey Stamen & William Costello
Datamation, May 1981
- 322 **An Untapped Resource: Government Data Bases**
Victor Block
Infosystems, July 1982
- 325 **Distributed Databases: Decisions and Implementations**
Robert Holland
Data Communications, May 1982
- 334 **Database Systems for Local Nets**
Eugene Lowenthal
Datamation, August 1982
- 339 **Data Base Machines—It's About Time!**
Frank J. Malabarba
Naval Data Automation Command
- 9 Telecommunications/Networks**
- 347 **Telecommunications: A Bloody Battle for the Future**
Charles W. Newton
Data Management, April 1982
- 353 **Local Networks: Making the Right Connection**
John Seaman
Computer Decisions, June 1982
- 371 **Comparing the CBX to the Local Network—and the Winner Is?**
George M. Pfister & Bradley V. O'Brien
Data Communications, July 1982
- 376 **Distributed Systems and Data Management**
Paul R. Hessinger
Datamation, November 1981
- 380 **Data Communications Ends Machine Isolation**
Dale Zeskind
High Technology, July/August 1982

10 Hardware

- 385 **A Look Into the Future: Are Mainframes Crumbling From Outside Pressures?**
Frederick W. Miller
Infosystems, July 1982
- 390 **Pushing the Limits of Magnetic Disk Technology**
Robert C. Schmidt
Data Management, July 1982
- 393 **Performance Improvements Boost Drum Memory Use**
William P. Riefenstahl & William Keith
Data Management, July 1982
- 396 **Perpendicular Could Be Right Angle for Future Memories**
Data Management, July 1982
- 400 **Videodiscs and Optical Data Storage**
Dick Moberg & Ira M. Laelsky
BYTE, June 1982
- 406 **Win with Winchesters**
Leonard Bleininger
Computer Decisions, June 1982
- 408 **Lasers Store a Wealth of Data**
Jeff Hecht
High Technology, May/June 1982
- 416 **Talk Is Getting Cheaper**
Paul Masters
Datamation, August 1981
- 419 **Voice Response Systems**
L. J. Foss
Data Management, August 1982
- 421 **Hedging Your Bets**
Samuel Feldman
Datamation, June 1980

11 Microcomputers

- 429 **Everything You Ever Wanted to Know About Microcomputers (But Didn't Know Who to Ask)**
Leland W. Slater
Navv Regional Data Automation Center, Norfolk
1 June 1982
- 450 **Corporate Brainchild—Microcomputers, Part 1**
Steven F. Hesprich
Journal of Systems Management, August 1982
- 455 **Corporate Brainchild—Microcomputers, Part 2**
Steven F. Hesprich
Journal of Systems Management, September 1982
- 459 **How Personal Computers Can Backfire**
Business Week, July 12, 1982
- 461 **Make Way for Micros**
David Whieldon
Computer Decisions, June 1982
- 471 **You Mean I Can't Just Plug It In?**
Peter Krass & Hesh Wiener
Datamation, September 1981
- 475 **Working Toward Standards in Graphics**
Fred E. Langhorst
Computer Design, July 1982
- 479 **A Generation Meets Computers or the Playing Fields of Atari**
Paul Trachtman
Smithsonian, September 1981

12 Office Automation

- 493 **IRM vs. the Office of the Future**
John J. Connell
Journal of Systems Management, May 1981
- 498 **The Mechanization of Office Work**
Vincent E. Giuliano
Scientific American, September 1982
- 508 **Replacing the Pad and Pencil**
Amy D. Wohl
Datamation, June 1980
- 511 **Is there an "Office of the Future" In Your Future?**
Jean S. Doremus & Michael G. Morgan
Journal Of Systems Management, July 1982
- 517 **Implementing Automated Office Systems**
James C. Wetherbe; Charles K. Davis; & Charlene A. Dykmen
Journal Of Systems Management, August 1981
- 524 **Rethinking Office Automation**
Raymond R. Paniko
Administrative Management, July 1982

13 Captain Grace Hopper, USNR

- 531 **Grace Hopper - A Living Legend**
Steve Johnson (J02)
All Hands, September 1982
- 535 **David and Goliath**
Grace M. Hopper, CAPT, USNR
Computers In The Navy
- 543 **Author Index**
- 545 **Title Index**
- 547 **DOD Computer Institute**
Course Information

REF-RL

radio liberty research

RL 454/83

December 6, 1983

ADMINISTRATIVE SURVEILLANCE--A MEANS OF POLICE REPRESSION*

Lev Yudovich

After Brezhnev's assumption of power, responsibility for stepping up internal repression was put in the hands of the USSR Ministry for the Maintenance of Public Order created in July, 1966.¹ The powers of this ministry were considerably broadened, while the legal guarantees of an accused person were reduced.² The attack on civil rights, freedoms, and legal guarantees was carried out under the slogan of intensifying the struggle against "antisocial manifestations," in other words, all manifestations of dissatisfaction with the Soviet regime. The newly created ministry and its local organs were given the task of carrying out administrative surveillance of persons freed from places of confinement and exerting "the necessary influence" on them. This amounted, in practice, to extending sentences by purely extralegal (administrative) police methods.

The Brezhnev regime found it necessary to take this step because the RSFSR Criminal Code that came into force on November 1, 1951, (and the criminal codes of other republics) had reduced the maximum terms of deprivation of freedom from twenty or twenty-five years³ to ten or, in the case of especially grave

* Translation of RS 228/83.

1. See Decree No. 594 of the Presidium of the USSR Supreme Soviet of July 26, 1966 (Vedomosti Verkhovnogo Soveta SSSR, No. 30, 1966).

2. For example, Decree No. 595 of the Presidium of the USSR Supreme Soviet "On Increasing Criminal Liability for Hooliganism" (Vedomosti Verkhovnogo Soveta SSSR, No. 30, 1966) replaced the normal preliminary investigation with a speeded-up administrative investigation.

3. Article 28 of the RSFSR Criminal Code of 1926 as amended by decrees of the Presidium of the USSR Supreme Soviet of June 4, 1947 (Vedomosti Verkhovnogo Soveta SSSR, No. 19, 1947).

crimes and especially dangerous recidivists, fifteen years.⁴ The consequence of this reform was to reduce the population's fear of the state. It turned out that, without draconian criminal laws, the regime could not protect itself, so a new punitive policy was embarked upon.

The creation of the new ministry was accompanied by the publication of a decree of the Presidium of the USSR Supreme Soviet "On Administrative Surveillance by Police Organs of Persons Released from Places of Confinement" and "The Regulations for Administrative Surveillance by Police Organs of Persons Released from Places of Confinement."⁵ The regulations defined the categories of people to be placed under surveillance: especially dangerous recidivists; persons sentenced to deprivation of freedom for grave crimes whose behavior while serving their sentences in places of confinement did not meet with the approval of the camp authorities; and persons sentenced to deprivation of freedom for grave crimes who, having served their sentences (or having been conditionally released), "continue to lead an antisocial life." In other words, administrative surveillance was imposed on the majority of convicted persons, including all those convicted of political crimes.

The regulations revealed the nature of this administrative surveillance: a ban on leaving home at certain times; a ban on frequenting certain places in a given raion or city; a ban or limitations on leaving a given raion or city; and a requirement to report to the police between one and four times a month.

To carry out administrative surveillance, police powers were sharply increased. Not only was the police given the right to impose administrative surveillance on the basis of material of its own to which the person under surveillance was not privy, but it could also extend the term of surveillance "until the expunging or removal of the record of conviction."⁶ Bearing in mind that it can take from three to eight years for the record of a conviction to be expunged and that the record of conviction for certain crimes is never expunged,⁷ it is easy to appreciate that

4. Article 24 of the RSFSR Criminal Code of 1960.

5. Decree No. 597 of the Presidium of the USSR Supreme Soviet (Vedomosti Verkhovnogo Soveta SSSR, No. 30, 1966).

6. Ibid.

7. See Article 57 of the RSFSR Criminal Code as amended by the decree of the Presidium of the RSFSR Supreme Soviet of September 14, 1969 (Vedomosti Verkhovnogo Soveta RSFSR, No. 47, 1969).

the police gained the power to impose long terms of administrative surveillance, in some cases lasting to the end of a person's life.

The police were obliged to keep a file on every person under surveillance. In it were gathered and stored information on the behavior of the person under surveillance received from the administration at his place of work, from organizations at his place of residence, and from individual citizens; information on the moral education talks conducted with the person by a policeman at his place of work in the presence of the administration, representatives of public organizations, or relatives; and information on the person's activities by day and night at home. To collect this information, the police was authorized to visit the person's residence at any time of day or night.

The idea of introducing administrative surveillance in the Soviet state was borrowed from the arsenal of the Russian Tsars. Under the old Russian legislation, police surveillance consisted of: restriction of the freedom to choose a place of residence, or a ban on living in certain places, or a restriction on freedom of movement for a period of between two and five years or even for life. Surveillance was carried out both openly and clandestinely. The purpose of police surveillance was openly declared to be the prevention of crimes against the state. In 1895, police surveillance was extended to all "persons considered harmful to the public order." Persons under surveillance could not be in government or public service. They were forbidden to teach, to keep printshops, or to sell books. The Ministry of Internal Affairs could forbid them to receive private mail or telegraphic communications.⁸ All of these restrictions have been included in Soviet administrative surveillance.

Since the regulations for administrative surveillance came into force in 1966, they have been amended three times, in 1970, 1981, and 1983.⁹ The latest of these amendments affected not only the regulations themselves but also Article 49 of the Principles of Corrective Labor Legislation, which had come into force in 1969.¹⁰ The decree incorporating these amendments was signed personally by Yuri Andropov. Like earlier amendments, they were aimed at broadening both the range of persons liable to administrative surveillance by the Ministry of Internal Affairs and also the grounds for imposing it.

8. Entsiklopedichesky slovar', Brokgauz and Efron, Vol. 20, pp. 432-34.

9. Vedomosti Verkhovnogo Soveta SSSR, No. 24, 1970, Article 206; No. 10, 1981, Article 32; No. 39, 1983, Article 584.

10. Vedomosti Verkhovnogo Soveta SSSR, No. 29, 1969.

Article 2 of the regulations of 1966 provided for administrative surveillance of three groups: especially dangerous recidivists; persons sentenced to deprivation of freedom for grave crimes "whose behavior while serving their sentences in places of confinement demonstrated a strong reluctance to embark on the path of correction and take up a life of honest labor"; persons sentenced to deprivation of freedom for grave crimes who, "after serving their sentences or being conditionally released, systematically violate public order and the rules of Socialist community living and, despite warnings from the police, continue to lead an antisocial way of life."

In 1970, the range of persons to whom administrative surveillance could be applied was extended to include "persons sentenced more than twice to deprivation of freedom for any premeditated crime." In 1983, it was again extended to include persons released from places of confinement either conditionally or conditionally with the obligation to work before completion of their sentences who commit a further premeditated crime during the unserved part of their sentence or during the period of compulsory labor.

The regulations of 1966 established the following grounds for imposing administrative surveillance: a) in respect of especially dangerous recidivists: a legally valid court sentence; b) in respect of persons sentenced to deprivation of freedom for grave crimes: the conclusion of the administration of a camp (or other corrective labor institution) and the supervisory commission that it was necessary. In respect of persons released without administrative surveillance being imposed, such surveillance could be imposed on the basis of material available to the police at a released person's place of residence.

In 1983, the administrations of corrective labor institutions--i.e. organs of the Ministry of Internal Affairs--were given the right to impose administrative surveillance without consulting the supervisory commission. Since October 1, 1983, the administration of a corrective labor institution has simply had to "coordinate" its decision with the supervisory commission. The most substantial change in the regulations is, however, the addition to Article 16 of a rule stating that:

persons under surveillance who leave their place of residence without permission to evade administrative surveillance and persons who, without valid reason, fail to appear at their chosen place of residence at the appointed time, in cases when administrative surveillance has been imposed on release from a place of confinement, are liable to criminal

prosecution according to the procedure laid down by the legislation of the Union republics.

The nature of this "new procedure" is revealed by Decree No. 1334 of the Presidium of the RSFSR Supreme Soviet, which supplemented two articles of the RSFSR Criminal Code. Article 198-2 now allows persons under administrative surveillance to be sentenced to between one and three years deprivation of freedom for leaving their place of residence without permission to evade administrative surveillance or for failure, without valid reason, to appear at the chosen place of residence. The decree was published on September 13, 1983, although the decree of the Presidium of the USSR Supreme Soviet proposing amendments to the legislation on administrative surveillance was only dated September 22, 1983. Thus, Mikhail Yasnov, the chairman of the Presidium of the RSFSR Supreme Soviet, acted even before the measure had been officially sanctioned at the all-Union level.

All this demonstrates once again the way in which Andropov, Yasnov, and their like flout the constitution by issuing decrees as and when they will. The anticonstitutional nature of the legislation on administrative surveillance with all its amendments and of the institution of criminal liability for violation of the rules of administrative surveillance is particularly evident when reference is made to Article 49 of the USSR Constitution of 1936 and Articles 121 and 122 of the USSR Constitution of 1977, which state that only the Supreme Soviet is empowered to enact new laws. The Presidium of the Supreme Soviet may interpret laws or, when necessary, amend them, but it is not entitled to enact new laws in the guise of amendments.

Routinizing the Discovery of Secrets

Computers as Informants

GARY T. MARX
NANCY REICHMAN
Massachusetts Institute of Technology

The king has note of all they intend
By interception which they dream not of.

—William Shakespeare, *The Life of Henry V*

- A computer cross-check resulted in the investigation of a California woman suspected of bilking the welfare department out of more than \$4,000,000. Using a variety of aliases over a seven-year period she successfully filed fraudulent assistance claims for 38 nonexistent children.
- The Commerce Department, concerned over illegal exports, has distributed a list of 12 "red flag" signals that may suggest an illegal transfer of goods. A 24-hour-a-day telephone hotline has been established. Persons working in high-technology industries are encouraged to report any suspicions.
- The FBI and IBM jointly run a fake consulting firm in the Silicon Valley in San Jose, California. The sting operation involves selling IBM trade secrets to Hitachi and Mitsubishi.

These diverse examples are typical of recent efforts to solve a traditional problem faced by any enforcement agency: the need to locate infractions.

Police in the United States traditionally have relied heavily on unsolicited information from citizens to direct their efforts (Black, 1980, Reiss, 1971.¹ In a democratic society there is much to be said for this means of mobilization. It can offer a degree of citizen control over police discretion. This, along with other limitations on the autonomy of police to initiate investigations, is surely a necessary feature of liberty.

The traditional citizen-reporting approach may work well where there are clear victims or observers who are aware that infractions have occurred and who are willing to report what they know. It is less

effective when those with information are intimidated or otherwise not forthcoming. When witnesses are not even present, when there is no clear individual victim, when the offense is hidden or highly technical, or where a well-organized conspiracy is present the traditional approach is irrelevant.

Reliance on citizens for information can have two major drawbacks: (1) the ratio of offenses citizens choose to report, relative to those they actually know about, may be too low or may be systematically biased in an undesirable direction; (2) there are many offenses of which citizens are unaware. These drawbacks have become more apparent in recent decades. In response, an important area of criminal justice reform has sought to improve the ability of social control agents to discover offenses and offenders systematically.

REFORMS INTENDED TO IMPROVE THE DISCOVERY PROCESS

Systematizing or routinizing discovery has taken two broad forms. One form responds to the problem of underreporting. It seeks to structure the environment so that citizens will be more likely to come forward with information. Toll-free hotlines where citizens may anonymously call in tips, televised police appeals for information, neighborhood crime watches, and citizen patrols seek to make reporting easier and more accessible and to increase the flow of information to police.² Protections for those who report have also been enhanced.³

The second form of enhancing information discovery involves police taking initiatives to discover infractions on their own, without being dependent on what citizens may choose to report. Undercover work is an example. Police increasingly have sought to discover crimes by becoming a party to them, whether as fellow conspirators, observers, or victims (Marx, 1982). Another form of police initiative we have chosen to call "systematic data searching." As illustrated by the discovery of the California woman who fraudulently received welfare aid for 38 non-existent children, systematic data searching involves gleaning data, usually in computerized form, for direct or indirect evidence of infractions.

While it would be worthwhile to devote equivalent attention to each attempt at enhancing the discovery process, we have chosen,

instead, to use this limited space to explore systematic data searching in greater detail.⁴ We do this because of its relative newness, its rapid expansion, and its having received little research attention. While considerable attention has been devoted to the vast new crime opportunities computers offer (Parker, 1976; Whiteside, 1978), less attention has been given to the role of computers in discovering crimes.

Systematic data searching involves more than just the application of computer technology to existing law enforcement process.⁵ It is in some ways a new tool. It permits the joining of heretofore independent pieces of information in order to expose offenses and offenders that would remain hidden unless such links could be drawn. Systematic data searches do not merely expedite existing discovery processes. They offer an entirely new means of exposing rule breaking. They offer a "value-added" or inductive method that differs from traditional, deductive methods. Rather than drawing inferences from a "crime scene" that has natural, seemingly self-evident boundaries, systematic data searching permits investigators to construct criminal scenarios from disparate data and events. They may also permit a form of statistical surveillance.

This article draws on 8 interviews with specialists in computer detection and over 100 interviews carried out in the course of our research on undercover tactics and insurance fraud investigations. Information from these interviews is not presented quantitatively, nor is it used to test hypotheses. Systematic research is premature until issues have been framed and questions raised. It is hoped that our discussion can contribute to the type of systematic research required to answer the questions to be suggested.

A MORE DETAILED LOOK AT SYSTEMATIC DATA SEARCHING

Systematic data searching has been facilitated by new computer developments. These developments have occurred concurrently with the increased prominence and attention given to what can be called "low-visibility" offenses. Much white-collar crime, such as price fixing, corruption, and trade violations, can be so characterized. The significant expansion of benefits provided by the modern welfare state has also generated new opportunities for fraud. The implications of this for exploitation have rarely been noted.⁶

Factors that inhibit the discovery of such offenses go far beyond the physical barriers and the right to privacy noted in the literature as factors that limit the discovery of offenses by routine patrols of public areas (Stinchcombe, 1963; Mawby, 1981). The impersonal and routine settings in which these offenses occur and the very large numbers of potential offenses/offenders means that control agents usually cannot rely on prior reputation as a means of suspicion, as they can with more traditional offenses.

Many crimes by or against organizations are deceptively masked as legitimate organizational transactions. Applying for and receiving welfare benefits, for example, is legal unless the fact of employment is concealed. Similarly, filing a property insurance claim is legitimate unless there was no loss. Since the infractions occur in the context of many similar, legitimate transactions, they do not stand out immediately as instances of wrongdoing. Organization members and routine organizational process also may shield illegal action from exposure.⁷

In such cases the legitimate and routine appearance of the violations is in sharp contrast to predatory crimes (such as robbery, assault, or rape) or even victimless crimes (narcotics, prostitution) where the apparent act is illegal and traces of the activity (the injured victim, the smashed window) are instantly obvious if seen. No similar "on-site" clues alert social control agents that low-visibility offenses have occurred. There is no "smoking gun."

Beyond their entrenchment in routine organizational process, low-visibility offenses often are difficult to discover because they occur over time and information about them is dispersed across institutional settings. The discovery of low-visibility violations that occur over time, or across agencies or cases, is enhanced by the pooling of information. Death records are a good example. Although they have major bearing on many federal entitlement programs, death records are maintained locally. Historically, there has been no systematized way for federal agencies to obtain these records automatically to confirm program eligibility. In addition, technical advances such as automatic check writing and depositing may further mask discovery. The system grinds along on its own initial momentum, absent an order to decrease.

Systematic data searches appear well suited for the exposure of these types of low-visibility offenses. In their simplest form searches may be applied to a single body of data. Before computerization, records such as applications were checked for internal consistency,

errors, and missing information. But this was often done superficially, with little cross-checking and in an inconsistent and nonsystematic fashion. The individual clerk or auditor usually had vast discretion over whether or not, and what, to check.

With computerization screening can become routinized, broadened, and deepened. Computers permit forms of investigation that previously were impractical. In contrast to traditional techniques that could assess static demographic data, computers permit analysis of more complex transactional data, such as number of visits to a doctor, phone calls to particular individuals, travel patterns, bank deposits, and the timing and interrelations of events (Burnham, 1983). A much more textured or dimensional picture is possible.

An internal computer data search may reveal discrepancies, contradictions, and irregularities that would be missed by a clerk reviewing the form. Equity may be increased as all forms are checked, not just those that happen to catch the fancy of an auditor. The IRS, for example, now is able to screen the over 90 million tax returns it receives for missing information and mathematical errors. Cross-referencing distinct data bases (as with social security numbers and death records) may expand and qualitatively change the nature of the search. Data analysis may yield profiles of likely offenders. Patterns of offense may be discovered through aggregation not possible if one follows a Sherlock Holmes logic of deduction and looks at only a few cases. Indicators may be created that suggest that a violation is likely. The investigator may then follow or track these cases over time.

Two increasingly prominent types of computerized data searching are *matching* and *profiling*. These certainly do not exhaust all forms of searching, but they are among the most important.⁸ While they may overlap or appear sequentially, they are analytically distinct and offer one way of organizing the empirical material.

MATCHING

Matching involves the comparison of information from two or more distinct data sources. It may be used for cross-checking and verification or to discover inconsistencies and multiple listings suggesting violations. According to one estimate, approximately 500 computer matching programs are being carried out routinely at the state and federal levels (U.S. Senate, 1982: 20).

Among the most dramatic examples of the violations matching may discover are impersonation and false representation. For exam-

ple, a cross-check of social security rolls and medicare records resulted in the arrest of 29 people for cashing checks made out to dead friends and relatives. One woman had been forging the name of a deceased friend for 14 years. Officials reported uncovering losses of over \$30 million (*New York Times*, May 20, 1983).⁹ In what a prosecutor called "the most concerted effort yet not simply to respond to complaints but to affirmatively go out and detect fraud," the U.S. Office of Education has used computer searches to flag suspicious applications in federal student loan programs. The rate at which fraud has been uncovered as a result has more than tripled (*Boston Globe*, June 27, 1983).

Third parties may exploit what once was a valid claim. For example, matching black lung program payments with social security records revealed that the program was continuing to provide compensation to 1200 individuals listed as deceased (U.S. Department of Health and Human Services, 1981: 24).

A second type of violation commonly discovered is "double dipping." A person may be legitimately entitled to the benefit in question, but, through seeking the same benefit in different jurisdictions, or using different names, or (where payment legitimately terminates) reapplying after an extended period of time, he or she may fraudulently obtain additional benefits. For example, a match of the welfare rolls of 34 jurisdictions involving 5 million records turned up 3500 cases where persons appeared to be receiving public assistance in more than one state (U.S. Department of Health and Human Services, 1981: 30). Some welfare systems will automatically cross-check birth records whenever a person claims to have twins, since false claims regarding twins are a well-known means of seeking increased benefits (*New York Times*, August 3, 1982).

Computer matching may also be used to discover false claims that would render an applicant ineligible for the benefit in question. For example, in Massachusetts computer matching has been used to find welfare recipients with bank deposits in excess of the amount permitted. The welfare department supplied banks with the names and social security numbers of all welfare recipients. Matching these numbers with their customer information, the bank officials gave the state a list of welfare recipients holding cash assets in their banks. The inquiry discovered over 1600 instances in which assets in excess of the \$5000 limit appear to have been held (U.S. Senate, 1982: 240).

The fraudulent claim may involve an event rather than some aspect of a person's biography. A common form of insurance fraud

involves purchasing the title certificate for a wrecked car sold as salvage. The car is insured and subsequently reported as stolen. Theft insurance would then be collected on a nonexistent car. However, with computer matching this has become more difficult to do. The National Auto Theft Bureau now maintains records of all vehicles sold as salvage and/or reported stolen.¹⁰ By marrying theft reports with salvage records, the computer matching program permits instantaneous discovery of a type of fraud that previously lay hidden in two rarely connected bodies of data.

Matching may be used to identify persons who fail to meet an obligation. For example, in an effort to discover income tax evasion, particularly by the self-employed, the IRS is testing a system that matches tax records to estimates of income based on the type of neighborhood an individual lives in and the type of car he or she drives. The data are to be purchased from private marketing firms that sell computerized lists to direct-mail companies. The IRS is also matching data from county recorders of deeds with tax returns, to find individuals who fail to pay capital gains taxes owed from the sale of real estate (New York Times, August 29, 1983).

Matching can also be used in a preventive way, for example, linking the failure to meet an obligation with a new request. In rules announced by the Office of Management and Budget in 1983, federal agencies are now prohibited from making loans, procurements, contracts, or major grants until they have prescreened applicants through credit bureau inquiries to be sure that they are not delinquent in repaying prior government loans and other overdue obligations (New York Times, September 24, 1983).

PROFILING

Matching may be used to construct profiles of violations or violators. But the logic of profiling is more indirect than that of matching. It follows an inductive logic in seeking clues that will increase the probability of discovering infractions relative to random searches.

Profiling permits investigators to correlate a number of distinct data items in order to assess how close a person or event comes to a predetermined characterization or model of infraction. The modal characteristics and behavior patterns of known violations or violators are determined relative to the characteristics of others presumed to be nonviolators.¹¹ Indicators of possible violations are developed from

this comparison. Where the behavior is complex and evolves, a model may be developed of the interrelations among the relevant factors. But most common is a simple laundry list of "red flag" characteristics. As more and more of these occur the case in question becomes more suspect. A second, more in-depth, investigation is then carried out to determine if a case that has been flagged as suspicious actually involves the violation.¹²

Profiling is indirect because the indicators used are not in themselves indicative of illegality. However, their joint appearance is thought to be associated with an increased probability that a violation will occur or has occurred. Profiling may be *singular* or *aggregative*. The former consists of a model of distinct attributes. The latter consists of the reappearance of factors that, appearing only once, in and of themselves would not trigger suspicion. Their appearance across cases, such as a single person's being the owner of several inner-city buildings that burn down, would lead to further investigation.

Let us consider singular profiling first. It focuses on discrete characteristics or events. There is nothing illegal or exceptional about being a male, purchasing a one-way airline ticket, paying for it with cash, and obtaining the ticket at the last minute at the airport. But analysis suggests that when these factors occur together, the chances of a skyjacking attempt are increased. The same thing applies to a drug courier profile used to stop suspicious persons at airports.

The IRS was an early user of profiles in efforts to identify tax violators. Persons claiming deductions beyond a certain percentage of their income and certain configurations of deductions are likely to trigger more detailed inquiry. One way to get on the IRS's "tax gap hit list" appears to be to purchase audit insurance (Wall Street Journal, June 29, 1983). The logic here is that people who purchase audit insurance are likely to have something to hide and are gambling that it's cheaper to purchase the insurance than to pay the tax.

Profiles also can be used in a preventive way. The development of arson early warning detection systems in Seattle, Boston, New Haven, and other cities illustrates this (National Legislative Conference on Arson, 1982). Computer-based arson prediction models are used to identify buildings thought to be at risk of being burned. This opens up the possibility that preventive action will be taken. In another form of prevention, the profile may result in interdiction before the act can be fully carried out. Airline skyjacking profiles are one example, for

instance, refusing to issue tickets to passengers matching the profile may prevent the skyjacking (Time, July 26, 1976). Interrogations and searches resulting from drug courier profiles are another example.

Profiles developed for identifying welfare fraud can be used to prevent ineligible cases from entering the system. For example, in Sacramento County (California) a profile for identifying suspicious cases has been developed around the number and age of children, health care, and school records. This model is based on an assumption of at least occasional childhood illness and treatment. If a recipient claims children and there are no school records and no medical claims for the children, further investigation results (U.S. Senate, 1982).

Profiles of auto theft and bodily injury fraud increasingly are used in insurance cases. Profiles are based on factors that often accompany fraud, such as losses occurring close to the inception date of a policy or claimants avoiding the U.S. mail in correspondence regarding the claim. A series of questions, a checklist of responses, and associated point system have been developed that allow adjusters quantitatively to rate the degree to which a particular claim is consistent with ideal fraud types (Reichman, 1983).

Aggregative profiling is based not on the distinctive characteristics of any one case, but on the frequency with which certain factors appear across cases. The profile emerges from the aggregation of similar incidents or configurations. There is an implicit threshold. Once this is reached, red flags appear. Aggregative profiling often is directed against systematic and repetitive violations rather than the one-time violation.

Such profiling has been used extensively in efforts to find insurance fraud. For example, the State of Florida's Division of Insurance Fraud maintains an index of all bodily injury insurance claims. The index is used to ferret out violations that cut across seemingly unrelated claims. Thus when the same doctor-lawyer combination reappears on a significant number of personal injury claims, investigators have reason to look further for a fake accident ring. This pooling of information may give the analyst reason for suspicion that would not appear to an insurance company office paying a single claim.

Similar logic underlies the Property Insurance Loss Registry (PILR), a not-for-profit discovery organization sponsored by the insurance industry. Among other information, it records the location of fires, insurees, mortgagees, and contractors. A current fire prompts a

search through the PILR index for other similar fires involving the same persons or organizations. While the discovery of other fires is not directly discrediting, it suggests that further inquiry into the fire loss is appropriate.

The Educational Testing Service uses a form of aggregative profiling to discover cheating. In 1982 the service sent out to takers of its scholastic aptitude tests about 2000 form letters alleging "copying." The letters note that a statistical review "found close agreement of your answers with those on another answer sheet from the same test center. Such agreement is unusual and suggests that copying occurred." Students are told that in two weeks their scores will be canceled and colleges notified unless they provide "additional information" to prove they did not cheat. A major factor triggering the sending of such letters is the "K-index," which compares incorrect answers among test takers (New York Times, July 2, 1983).

Profiling is also used in some parts of the private sector to identify drug users. For example, one drug consultant goes through computerized company personnel records looking for employees under 35 who show higher-than-average rates of (1) absenteeism, (2) requests for early dismissal or time off, (3) lateness, (4) sick leave, (5) accidents, and (6) Worker's Compensation claims. An employee showing sufficient elements of this profile may be asked to undergo a blood or urine test to determine the presence of drugs (Newsweek, August 22, 1983).

USES OF THE RESULTS

In the data analyst's language, the results of an initial computer search are referred to as "raw hits." Depending on search type, these include indications of direct infractions or a sufficient number of red flags alerting agents to possible violations. A name on both the welfare and city employment rolls, the repetition of an event or characteristic beyond some identifiable threshold (such as four consumer complaints against the same company), or a person or event that matches a profile associated with previous violations are illustrative. These raw hits include the total universe of hits. This universe in turn is made up of "solid hits," "misses," and "inconclusives."

"Solid" or "true" hits are instances in which conclusive evidence of violation is found.¹³ But what happens when additional investigation yields conclusions that negate the initial finding of a hit? In most

cases what appeared to be hits will simply be considered misses and it will be possible to explain away the initial suspicion. Misses appear as a result of errors, situational factors that lead to a different interpretation of the facts, or, in the case of profiling, a necessary casualty of probabilistic reasoning.¹⁴ In other cases, while sufficient evidence of infraction is not available, neither is the conclusion of a miss. No evidence is found to cast doubt on the original reasons for suspicion, and evidence to strengthen it may even have been found. The term "inconclusive" is appropriate here. Where there is reason to think that a violation will eventually appear, one response is to monitor or track a case over time.¹⁵

The goals of a data search may change with its repeated use. When a system is first applied to an existing data base, its goal is likely to be the discovery of current or past offenses. It may seek to "weed out" bad apples. It searches for illegitimate cases. For example, recipients of the black lung benefits are provided with payments for children up to the age of eighteen. When the U.S. Department of Health and Human Services screened its records, it found 3000 offspring whose ages exceeded the eligibility standard, though not all of these were continuing to receive payments (U.S. Department of Health and Human Services, 1981: 25). The statistical technique of discriminant analysis is used by the Farmer's Home Administration to identify problem loans. Based on patterns identified in previous cases of default and foreclosure, the technique permits investigators to screen out current loans exhibiting those characteristics associated with a high probability of default (President's Council, 1983).

Once a data base has been purged initially of such cases, however, the goal may shift to deterrence and prevention. In fact, preventing fraud and abuse before they occur is the new objective of the President's Council on Integrity and Efficiency (PCIE), established in March 1981 to promote and coordinate the activities of inspectors general, many of whom pioneered the use of computer matching. Program administrators hope that the publicity about data searching will deter potential offenders.¹⁶ Public relations efforts may seek to create the impression that the computer's awesome power is all knowing. This may build upon the mystique surrounding technology in general and computers in particular. Fear and trembling may be engendered among the naive, as they impute unrealistic powers to the computer. There is a parallel to the unwarranted power some persons impute to the lie detector. This is reminiscent of President

434 AMERICAN BEHAVIORAL SCIENTIST

Nixon's immortalized words on the Watergate tapes, "Listen, I don't know anything about polygraphs, and I don't know how accurate they are, but I do know that they'll scare the hell out of people."

Where such deterrence is not present, applying the search before people are officially entered on the rolls or, in the case of the black lung example above, assuming that they are removed at the appropriate time may anticipate violations and allow for preventive measures. In a private sector example, major credit card companies may soon be confirming the personal identity of credit card holders through signature verification technology. A technique has been developed for analyzing the pressure and direction of a signature as it is being signed. This could then be compared to data stored from previous signatures (Wall Street Journal, June 9, 1983).

SOME POLICY AND RESEARCH ISSUES

I hope you do not assume yourselves infallible of judgment when the most learned of the apostles confesseth that he knew but in parts and saw but darkly through a glass.

— Sir Richard Saltonstall

It is clear that data searching techniques such as matching and profiling can significantly enhance discovery. As we noted earlier, systematic data searching seems particularly well suited to ferreting out certain low-visibility offenses that involve organizational processing. As with undercover sting operations, their dramatic results make for good media treatment. These techniques generally have been positively received. Their use is expanding rapidly. But, as with any means, they have a cost. The lunch is never free, whatever other attractions it may have. Two of the most important costs are the consequences of error and the implications for civil liberties.

ERRORS

Important factors in the assessment of data searching are the cause, frequency, and consequences of various types of error. At least five sources of error can be identified: (1) erroneously reported or incorrectly entered data, (2) time lags, (3) computer hardware and

software problems, (4) the acontextual nature of the decision process, and (5) the probabilistic nature of profiling.

The extent of erroneously reported, or incorrectly entered, data will vary greatly across programs and data types. We know little about its frequency. A study of the social security numbers of over 2 million food stamp and AFDC recipients found 5100 instances in which nonissued numbers were in use. Approximately one-third of these cases were a result of data input errors — the numbers were transposed by the applicant or by program officials (U.S. Senate, 1982: 5). In the first computer run of the Massachusetts bank records match, 24% of the social security numbers used in the matches were incorrect (U.S. Senate, 1982: 224). A procedure adopted later, which coupled the first letter of the surname with the social security number, helped reduce errors based on incorrect matches to 7%. Although this is a significant reduction in the error rate, the ease and magnitude of such errors gives on pause.

The process used to create the data base must be seen to reflect human judgment and not be seen as a perfect reflection of reality. It must be approached tentatively. Were the data gathered under coercion or periods of great stress? Are data collectors and processors aware of proper data collection procedures and motivated to follow them?¹⁷ Do program staff have incentives for falsifying data? If matters of judgment are involved, how high is reliability across judges? Even when the agency that initially gathers the data discovers an error, the ease of access to computerized information on the part of other agencies may limit its ability to control the flow of erroneous information. The automatic interfacing of computer systems may mean that the original processors of the data are unaware of the ultimate users and uses of such information.

The time lag between events, the reporting of events, and input into computerized data banks and analysis offers another source of error. For example, in New York State a match of work records with a list of persons receiving assistance in the last quarter of 1978 revealed that 10% of welfare recipients were actually working. A second review disclosed that at least half these persons were on both lists legitimately. Some recipients had been on welfare during the beginning of the quarter and only subsequently found work. Because the data were not updated in a timely fashion, some innocent individuals were initially suspect (Boston Globe, July 23, 1979).

Computer hardware problems may lead to data errors. Among problems that can be caused by faulty hardware is the "doubling up of

records" so that the value of a variable is recorded twice. This can wreak havoc with quantitative eligibility requirements such as a minimum amount in the bank, age, or number of children. Such hardware problems are easy to correct technically once they are located. But this requires vigilance in looking for errors and the incentive to make corrections. In the interim, persons may experience loss of benefits or receive benefits to which they are not entitled.

Another not uncommon technical problem lies with software errors. In using large data bases formatting errors can easily occur. If a command has been formatted incorrectly, the wrong variable will be pulled out for analysis. For example, when applicants provide income data for several years, a formatting error could abstract a previous year's income for current income.¹⁸

The error sources considered thus far are largely technical. With sufficient experience, resources, cross-checks, updating, and incentives, they can probably be reduced to an acceptable minimum. But this may not be the case with errors that are related to substituting technical for human judgment and profiles based on samples for which the true parameters are unknown. The most serious questions raised by systematic data searching lie here.

When a machine recommends a decision, the recommendation is only as good as the data and programs that have gone into it. One measure of goodness has been considered above—whether the data are erroneous in some technical sense. But a more subtle meaning involves completeness and sensitivity to unique parameters. When used as a decisive guide, rather than as an aid, systematic data searching is misused. The machine should not be a substitute for human discretion and judgment.

Errors in interpretation may arise because of the acontextual nature of the data analysis. Only a fraction of reality's richness is abstracted out and put into machine-analyzable form. There is a bias toward general features characterizing many cases, rather than the atypical, idiosyncratic, or extenuating circumstance.

As we move from the formal and general categories used to develop aggregate patterns basic to the actuarial method, to inferences about particular persons in specific situations, problems may appear. An example of this can be seen in the case of a nursing home resident who lost her Medicaid eligibility as a result of the Massachusetts bank matching program described above. The data that resulted in her being dropped were technically correct as far as the

search program was concerned. Yet it was a wrong decision. The woman's bank account included a certificate of deposit held in trust for a local funeral director to be used for her funeral expenses. Although federal regulations exempt burial contracts from asset calculation, the trust was included in the determination of her assets and she was excluded from the program (U.S. Senate, 1982: 106-107).

In another case a Washington, D.C., welfare recipient obtained a job at the Department of Health, Education and Welfare. Although she properly notified the welfare department of her changed status, word never reached those responsible for mailing the checks. The checks kept coming despite her repeated attempts to inform the welfare department of her new status. She eventually cashed the checks to pay off doctor bills incurred as a result of her serious illness. Subsequently, she was indicted on a felony charge and her name (along with 15 others) was listed in local newspaper stories describing the results of HEW's computer matching of its own employee records. Many of the others indicted also had informed the welfare department that they were currently working. When the judge learned the details, a majority of the cases, including that of the woman described above, were dismissed or reduced to misdemeanors. Yet the damage to these people's reputations and six months of uncertainty before their cases came to trial cannot be undone.¹⁹

A final source of error inheres in the very idea of profiling. It stems from statistical reasoning and group comparisons. With aggregative profiling some hits composed of repetitive events will appear as a result of chance. For example, sometimes persons showing roughly equivalent error patterns at a test will represent random factors rather than cheating. Some persons may simply have the bad luck to have a series of fires on properties they own without arson as the cause.

The data base used for constructing a profile may be reasonably accurate as far as it goes, but may simply not be representative of the larger universe of events. Important data may never enter the system. Thus it is sometimes argued that our knowledge of criminals is distorted because it is based primarily on those who get caught and they may be less competent than those who manage to avoid apprehension.

When data gathering on controversial and confidential topics is separated from data analysis, users may not be in a position to know much about the representativeness of the data they are given. Prose-

cutors, for example, usually have no choice but to accept the selectively reported information police bring them on gambling (Reuter and Rubenstein, 1978).

Even in the unlikely event that a profile was to be developed that described characteristics of all true violators, it would also likely characterize many nonviolators. In the case of skyjackings, for example, a majority of skyjackers may fit the profile, but so too do a large number of nonskyjackers. Given the extreme rarity of skyjackings per airline passenger there are no doubt many more misses than true hits. This also may be true for airport drug courier profiles that include such criteria as arriving from a city noted as a drug source, casual dress, scanning the concourse, making a telephone call on arrival, and appearing nervous (U.S. v. Harrison, 1982). While the profile does turn up solid hits, it may also cause much embarrassment and inconvenience to those wrongly interrogated. Procedures for taking reparative action, to the extent that this is possible, are clearly appropriate.

Whatever the source, errors will occur. In considering their costs it is useful to separate errors involving false accusations from those involving the failure to identify violations. The common distinction used in the analysis of statistical data between Type 1 and Type 2 errors can be usefully applied here. Type 1 errors involve identifying an infraction when in fact none exists. Type 2 errors involve failing to recognize an infraction when one does exist.

Type 1 errors involve false accusations. Like the dolphins who are inadvertently trapped in nets put out for tuna, innocent persons are caught in the net thrown out for offenders. Loss of benefits, defamation of character, alienation, and a more general delegitimation can result from such errors. In the case of false accusation, the state has a moral, and often a legal, obligation to provide a means of review. Although Type 1 errors have an individualized impact, they may incur high societal costs as they challenge democratic ideals of fair process.

Type 2 errors reflect an inefficient discovery mechanism (that is, not netting the universe of offenders). Their consequences vary according to whether one seeks to discover infractions that have already occurred or those that are planned. Not identifying a direct violation (for example, that a person is obtaining public assistance while working) may be inefficient, but it does not produce a clear direct cost since the behavior would have remained hidden whether or not a weak search process were in place. On the other hand, as the case of arson or skyjacking suggests, when the goal is prevention, the failure to

recognize a set of behaviors or events as consistent with a profile of wrongdoing can have more serious consequences.

Type 1 errors almost always become manifest because the investigation reveals a miss or a falsely accused person protests. But whether or not Type 2 errors are identified varies across offense types. Such errors are likely to be discovered only if a victim reports the offense or if it of necessity becomes public. For example, skyjacking offers a great contrast to drug smuggling. With a profile in place every skyjacking attempt represents a Type 2 error. But completed drug smuggling violations are far more difficult to identify. The extent of Type 2 errors involving the former can be checked continuously, but with drugs this is almost impossible. Where profiles can be checked they are subject to more frequent revision and, presumably, improvement. Where the size of Type 2 errors cannot be determined the profile remains a captive of its assumptions, which must remain unvalidated. The IRS, with the power to carry out in-depth investigations of random sample of taxpayers, illustrates one method of assessing the extent of Type 2 errors that would not otherwise be visible.

The assessment of errors also must consider the rate of error relative to the rate of true hits. If you increase the capacity to get true hits, do you proportionately increase the rate of errors or does the error rate grow exponentially? Or are there instances in which they might even be inversely linked?

In his novel *Nineteen Eighty-Four*, Orwell imagined a social control system that was both highly efficient and repressive. Perfect control over information was the key element (whether the ability to discover infraction or to manage beliefs). While not explicitly mentioned, computer technology was implied. Our review certainly does not question the repressive potential of such technology. But the sources of error we have noted clearly call into question limits on the efficiency and accuracy of computer control technology and illustrate the high cost of mistakes.

CIVIL LIBERTIES

Computer data searching involves the same civil liberties issues raised by the use of computer files in general.²⁰ Visions of the central all-knowing computer and Kafkaesque nightmares lurk on the horizon. Important concerns are privacy, Fourth and Fifth Amendment protections, and due process of law.

Critics argue that these searches are more intrusive than other forms because those subject to them are likely to be unaware that any search is going on. They may have given direct or willing consent for neither the search nor the disclosure of personal information to others. In cases in which consent has been given, this may be a result of duress and coercion rather than a real choice, since one may believe that one may have to forgo a badly needed benefit if one does not give consent.²¹

Privacy may also be violated by the improper disclosure of data to third parties without the consent of the subject. Or the data may be improperly obtained by them. The sharing of data across agencies heightens the risk of unrestricted or improper access to confidential information. Even without such exchanges, the fact that security around these kinds of data sets is generally weak invites abuse.²²

The use of computerized records for purposes unrelated to their initial collection has also been questioned. At the federal level such use is prohibited normally by privacy legislation. However, the Privacy Act of 1974 exempts computer matching programs when they are classified as "routine use" procedures, meaning when they are used for purposes compatible with the reasons for which the data were collected originally.²³ Broad interpretations of "compatible purpose" have made it possible to include nearly any government-initiated venture. The "routine use" classification can thus be used to circumvent protections against invasions of privacy the legislation was designed to prevent.

The programs may be questioned on Fourth and Fifth Amendment grounds. Searches can be viewed as "fishing expeditions," absent any substantial evidence of wrongdoing by the person in question. As such, they may be seen to violate the Fourth Amendment's protection against unreasonable searches and seizures. When data voluntarily given for one purpose are used for another, a person's right to protection against self-incrimination may be violated.

To the extent that one is not provided with proper notice that an individual is subject to a search, timely notice that one is a "hit," and an opportunity to contest the results of a search, due process questions also emerge.²⁴

In contrast to conventional criminal accusations, data searching may transform the presumption of innocence into an assumption of guilt. It can lead to imperious behavior as an agency cuts off benefits or cancels test scores without even a hearing. Accusations become

equivalent to convictions without a trial. The burden of proof may be on the target of the hit to show that the violation did not occur, rather than on the agency to show that it did. Officials may abdicate responsibility for their accusations to computer programs or models. In such cases suspects effectively relinquish their rights to face their accusers, at least directly.²⁵ Even then, challenges may be possible only after punitive action has been taken on, and publicity generated with respect to, the presumed guilt.

Supporters, however, argue that a balance must be struck between the rights of the individual and the needs of the state, and do not view matching programs as undue intrusions. Properly conducted computer searches are seen to be less intrusive than other forms of search, such as rummaging through a person's bank records. Data searches abstract specific variables from records, with total disregard of other variables. In contrast, an individual searcher can scan entire records picking and choosing among items. Furthermore, consent for computer searches is often given, or implied when one voluntarily provides the data. Advocates claim that with proper guidelines and administration, problems are minimal.²⁶

Thus far most of the debate between opponents and supporters has reflected competing value positions. It also has been at a very general level and has not made distinctions between types of search or error. Disagreements are now based primarily on value positions, with neither side able to examine adequately the empirical premises that bear upon the arguments. Given the absence of adequate data on most of the issues in question, it could hardly be otherwise. We have only minimal data on the extent of falsely accused people and the ratio of hits to misses for various kinds of searches. Little is publicly known about the validity of different profiles. Data on the frequency of the concerns raised by civil libertarians (or the counterclaims regarding the effectiveness of guidelines offered by supporters) are also missing. Nor do we have studies showing whether the discovery benefits continue over time or become neutralized with regular use.²⁷

We do not have the detailed case studies of the actual operation of matching and profiling programs that are requisite for sound policy recommendations. There has been little discussion of how risks can best be minimized and errors corrected or of how competing values should be weighed. How do matching and profiling differ from each other with respect to the costs of error? What are the relative costs of Type 1 (false accusations) and Type 2 errors (failing to identify an

infraction)? Should there be a presumption against using such techniques, or certain forms of them just as there is with the use of weapons or Fourth Amendment searches, except under special circumstances and when no other practical means are available? How does systematic data searching compare to other means of obtaining information on low-visibility offenses such as undercover tactics and efforts to increase citizen reporting?²⁸

As in so many other areas of contemporary life, rapid technological development has outpaced the establishment of ethical and legal standards for their use. The important Federal Privacy Act of 1974 does not address many of the issues raised by recent computer developments. Less than one-fifth of the states have laws requiring written standards for the collection, maintenance, and dissemination of person information, though this number is growing. Of course, as time passes and problems are identified the quality of computer use in the areas considered above will no doubt improve. But this is likely to be offset by problems associated with the continuing expansion of computers to new untested areas.

SOME THEORETICAL IMPLICATIONS

The significance of systematic data searching goes beyond the public policy questions considered above. It also has implications for understanding society and the nature of social control. The use of computers as informants is but a small part of a broad social process of rationalization.

The recent growth of matching and profiling is part of a more general process of rationalization that began in the nineteenth century. The same broad social forces affecting the economy touch criminal justice (Spitzer, 1979). In a rational effort to control the environment, policy has become more systematic and routinized. Social control has sought greater effectiveness, efficiency, certainty, and predictability.

Rather than having to rely on what citizens happen to report or police accidentally discover, control agents are taking greater initiative. This may bring greater equity as police seek independence from the biases a citizen-based reporting system may entail. With a skeptical and scientific ethos and a broad data base that can be inexpensively screened, it becomes prudent to consider everyone a possible suspect initially. Analysis rather than tradition becomes the basis for action.

Eliminating the traditional temporal distinction between locating an offense and searching for an offender may yield greater efficiency. Some systematic data searches collapse these processes as offense and offender are discovered simultaneously.

Yet, just as Mark Twain observed that claims of his death were greatly exaggerated, so too many claims about the efficacy of a rationalized criminal justice system be overoptimistic. In the case of systematic data searching, for example, if it does not contain within it the seeds of its own destruction, it at least contains an ironic vulnerability to its own neutralization (Marx, 1981). In any setting of strategic conflict, efforts at systematization (unless kept secret) can be exploited by skilled adversaries.³⁹

The certainty such techniques seem to offer may be illusive. Their advantages may be temporary or may result in a skewed population of apprehended offenders. Routinizing discovery procedures usually involves focusing attention on a limited number of indicators. These may be invested with far more predictive power than they warrant. Focusing attention on specific indicators implicitly diverts attention from other indicators and can result in tunnel vision.³⁹ The indicators chosen can easily come to be treated in a ritualized way. Enforcement agents may be held accountable for following correct procedures, rather than for the results of following those procedures. Only superficial concern may be given to whether or not indicators are valid or have been obtained or presented properly.

While deterring or discovering some offenders, routinization can offer an almost guaranteed means of unauthorized access to others, who gain knowledge of the system and take actions to neutralize it. Altheide (1975) has illustrated how security operations designed to restrict territorial access also can serve as a means for facilitating unofficial entry. The same holds for access to the benefits that systematic data searching is designed to control.

By learning what prompts a hit or a red flag, knowledgeable violators may take steps to avoid them. Some variables used in matching and profiling can be manipulated or avoided easily. For example, the well-publicized match of welfare and bank records in Massachusetts no doubt led some persons to hide money in banks outside the state, to entrust it to others, or to convert assets to a different form.

A different type of neutralization lies in the use of false names and identification numbers. Basic to some contemporary matching is discovering the same name, identification number, address, and the

444 AMERICAN BEHAVIORAL SCIENTIST

like on lists that should be mutually exclusive. This can be avoided through the use of false identification.³¹ The name, identification, or record presented may be valid but may simply not belong to the person presenting it. A record check may attest to the validity of the record, but it is unlikely to discover that it does not legitimately belong to the person presenting it.

Publication of the characteristics used to profile arsonists or skyjackers may offer such persons a way to avoid detection. The likelihood of the discovery of an arson pattern through the Property Insurance Loss Registry described above is reduced if each property is in a different and unrelated name. In response to five skyjackings to Cuba in a two-month period, the Federal Aviation Administration is considering changing its behavior profile (New York Times, July 7, 1983).

Awareness of this neutralization potential raises questions about who is likely to get caught in a routinized discovery system. Clearly, not all potential offenders can acquire the knowledge, or have the skill, sufficient to neutralize the system. However, over time it seems likely that these systems will disproportionately net the marginal, amateur, occasional, or opportunistic violator, rather than those who are more systematic, repetitive, skilled, or professional in their rule breaking. The latter ironically may be granted a kind of license to steal, even while headlines hail the effectiveness of control agents using new techniques.³² To be sure, where costly violation of the public trust or serious crimes are involved, any apprehension may be desirable. But the routinization of discovery does raise a type of equity issue rarely heard. The question is not the familiar one of how authorities use their discretion in deciding what laws to enforce or who to go after, but, given the means they use, what kinds of cases they are likely to discover.³³

Beyond questions of equity, efficiency, and the cyclic and dynamic nature of rule enforcement and violation, there is a broader question about the reach of social control. Observers such as Foucault (1977) view an irreversible continuing historical process of more intensive and extensive social control. The capacity of the modern state to gather information and to punish is seen to extend ever deeper into the social fabric. Control is based on "observation, surveillance, and inspection" rather than primarily on physical coercion. Conformity is

thought to emerge out of fear of a pervasive and omnipresent panoptic eye. The net has widened and the mesh thinned (Cohen, 1979). While computer matching and profiling may seem to be relatively pale and benign variants of this, variants they are.

How far do we want those in authority to go in their power to discover infraction? In a time of strong citizen concern over crime and the increased prevalence of low-visibility offenses, there is a great deal to be said for enhancing this ability. The proportion of offenses discovered by police relative to those reported by citizens is increasing.

Yet there is another side as well. A different version of the equity problem may appear when there is a gap between the knowledge of violation and the ability to sanction. While ignorance is not bliss, there is a certain wisdom to the inability of the three monkeys to see evil when action cannot be taken with respect to it. Powerful new discovery means may overload the system. Authorities may discover far more violations than they can prosecute or process. This overabundance can lead to the misuse of discretion and demoralization. Charges of corruption and favoritism may appear and the system may be perceived as unfair.

If this were all that was at stake, awareness of the potential problems and well-conceived policy for structuring choices might suffice. But there is a more onimous side. Paradoxically, *both* repression and equal law enforcement may be inhibited when authorities lack information. As Selznick (1948: 84) observes:

Do we need or want agencies of control so efficient and so impartial that every actual offense has an equal chance of being known and processed? . . . I am concerned that we do not respond too eagerly and too well to the apparent need for more effective mechanisms of social control. In the administration of justice, if anywhere, we need to guard human values and forestall the creation of mindless machines for handling cases according to set routines. Here vigilance consists in careful study of actual operations so that we may know what will be lost or gained.

Systematic data searching, along with the new citizen reporting programs, undercover police practices, electronic surveillance, and other technical means, offers compelling and little understood arenas for such study.

NOTES

1. We are defining "police" very broadly. By "police" we refer to those charged with the policing function, regardless of what the formal title is. All persons who enforce rules must confront issues around the discovery of their violation.

2. Such programs do generate information. For example, a Baltimore call-in radio program, "Report a Pusher," led to 91 arrests on drug charges. During the 4-hour program, police appealed to citizens for information on drug trafficking. Off the air, detectives took calls and recorded names, license numbers, and other information about persons callers suspected of being involved in narcotics transactions (New York Times, November 7, 1982). In Michigan, \$1000 is offered for information leading to the arrest and conviction of arsonists. From the inception of this reward system in 1975 to 1981, 26 payments were made (Arson News, 1981). What is not usually considered is how much of the information provided would have been forthcoming even in the absence of such programs.

3. Thus federal and in many places state legislation and judicial decisions have offered new protections for whistle-blowers. The Federal Witness Protection Program provides relocation and a new identity to informants (see Montanino, this issue). Legislation has also introduced negative sanctions for *not* reporting things such as child abuse and certain hazardous working or environmental conditions.

4. The methods are not mutually exclusive. For example, a lead generated by a hotline or a computer search may lead to an undercover operation. Computers, of course, are part of a broader family of rapidly developing technological means, including electronic surveillance and forensic science, also used to enhance discovery.

5. For example, it contrasts with a New York City program called "CATCH" (computer-assisted terminal criminal hunt) designed to streamline the identification of suspects. CATCH is a computerized "mug book" permitting quick retrieval of names of suspects who fit the description fed into the system. Computers have simply improved upon a traditional tactic (Computerworld, April 7, 1980).

In focusing on the discovery of offenses we are also referring to something beyond merely checking a second data base to find a person's address (such as the Selective Service's use of IRS data to locate people suspected of failing to register for the draft) or using that data base for sanctioning purposes, as with the state's garnishment of income tax refunds due to fathers who default on child support payments.

6. In 1959 entitlement programs accounted for 15% of the federal budget; in 1970 such expenditures had increased to one-third of the \$62 billion budget; by 1981 they were \$300 billion—almost half the budget.

7. See Katz (1978), Vaughan (1980), and Altheide and Johnson (1980) for discussions of the way task differentiation and bureaucratic organization can shield deviance and neutralize control.

8. Matching across data bases, which is one of our concerns here, shares much with the more traditional and common searching of a single data base. At an abstract level the correlation of distinct information involves the same logic of inquiry. But the former raises questions of privacy and data compatibility (which may have implications for errors and misinterpretations) not found when a single data source

belonging to the agency in question is used. Profiling, the second technique we consider, may draw upon single or multiple data sources.

While similar privacy issues are raised, matching is also distinct from simply looking at another agency's data for cases. For example, Skolnick and Woodworth (1967) have noted how police in Westville located cases of statutory rape from the files of other public agencies. In a British example, Mawby (1981) reports on police identifying drug users by monitoring hospital emergency room activities for drug overdoses.

9. It is well to note that all accounts of the dramatic success of such programs have come from advocates who carried them out. Whether an external audit and a careful figuring of costs and benefits would yield equivalent support is another matter. For example, the New York Civil Liberties Union (1982) argues that the unreported costs of New York State's wage-reporting system, a match of public assistance, unemployment records, and reported earnings, may add up to three or four times those officially stated, while savings may be far less than assumed.

10. This is a not-for-profit clearinghouse supported by insurance companies to provide information and assistance to the insurance industry and law enforcement.

11. Of course the profile is only as good as this assumption. Some in this group are undiscovered violators, though designers of profiles usually assume that this constitutes a small proportion.

12. Depending on whether the data offer direct or only indirect evidence of violation, matching may also trigger a more in-depth investigation. But the more in-depth investigation is always found with profiling.

13. The discovery of infractions, of course, is only the first stage in the enforcement process. How the information is used, and whether it is even used at all, are distinct questions that we will not consider here. Among actions that may result from discovery are prosecution, restitution, denial of a claim or benefit, public relations, blackmail or bribery, and entering into some form of exchange relationship with the violator, such as turning the person into an informer or witness. An overabundance of cases and disinterest, or bias on the part of the enforcement agent, may result in no action being taken. Or, in Silbey and Bittner's (1982) term, the "reservoir of un-enforced law" may be directed toward enforcement ends far from those intended by drafters of the original legislation.

14. Raw hits are less meaningful for profiling than for matching on average. Since profiles are based on statistical reasoning rather than the often binary and mutually exclusive categories (at least with respect to an agency's rules) of matching, far fewer solid hits are to be expected.

Efforts to make insurance rates and benefits "gender blind" involve some equivalent issues. While perhaps rational and fair in the aggregate, for any given case the prediction on which they are based can be wrong and unfair. The size of the comparative standard deviations can permit some estimate of the frequency of this.

Similar issues are raised by proposals to base sentencing on "career criminal profiles." A controversial Rand study (Greenwood, 1982), for example, proposed that courts use a profile of the career criminal in deciding the length of sentencing for convicted criminals. A person is presumed to be a high risk for a career in crime if he or she shows at least four of seven variables (for example, in jail for more than half of the preceding two years, previous conviction for the same crime, a record before the age of 16, or unemployed for more than half the preceding two years).

15. Interesting civil liberties and policy questions are raised about the intensiveness and length of time of such monitoring. The monitoring of a targeted person because of an inconclusive search can be separated from the routine monitoring that may occur when computers are part of the system being searched/monitored, rather than merely an instrument of the search. Discovery may be built into the work process. For example, an economic forecaster was arrested after it was discovered that he illegally tapped into a Federal Reserve computer in an attempt to obtain secret information about money supply. The computer recognized the tapping. The man was identified through a trace on his phone line (New York Times, January 5, 1983).

Social security field offices use a specialized "intelligence terminal" that records the author of all computer entries. This is used to monitor the work performance of data entry clerks, and can also be used as an audit trail (Wall Street Journal, July 7, 1982).

The completed input of records and the time they take to process can be logged, as can things such as the number of keystrokes for a given worker. In Massachusetts Blue Cross/Blue Shield claims offices a computer keeps track of worker productivity. Wages are adjusted every two months to reflect the output of data clerks (Kuttner, 1983).

The monitoring of a targeted person is also separate from the use of "computer software time bombs" that may automatically go off when a particular data configuration appears. For example, where personal biography intersects organizational rules in a predictable way, computers can be programmed to respond to changes in a person's status that affect eligibility for a benefit. Changes in age are a clear example.

16. For example, former Inspector General of the Department of Agriculture Thomas McBride, who was instrumental in establishing federal matching programs, reports that the publicity generated about a food stamp matching program resulted in a number of persons asking to be dropped from the program (U.S. Senate, 1982: 20). Whether all of these persons were ineligible or would have been discovered from the match is another question.

17. Criminal records, for example, offer an area where data quality leaves much to be desired. Laudon's (forthcoming) analysis of the FBI's automated criminal history file found that 54% of the records disseminated had data quality problems.

18. In a slightly different context, computer program errors may lead to erroneous medical diagnoses. The General Accounting Office reported that improperly programmed medical instruments have led to wrong diagnoses and at least one death (New York Times, August 22, 1983).

19. The failure to cut off a check once a recipient has reported a change in status represents a type of government-sponsored random integrity test of citizens (though this is not intended). This shows some parallel to indiscriminately applied undercover temptations. In both cases, according to the letter of the law, persons may be guilty technically. Money after all was taken, even if it was thrust upon the "guilty" party. But it is not clear that any broad social purpose is served by offering very attractive temptations to persons who may be weak and vulnerable, absent indications of prior wrongdoing on their part.

Advances in banking technology may unintentionally make it morally and technically easier for such fraud to occur. For example, Louise Van Vooren died in 1976. The government continued to send her social security checks directly to her bank for

automatic deposit until 1981. During that time her daughter drew on the money that was regularly deposited in her deceased mother's account. This seems to involve a lesser degree of moral turpitude than cases where the deceased's signature is forged directly on the social security check. As with the above welfare cases, should such unwitting government encouragement in a violation be treated the same way as more autonomous violations?

20. See, for example, Westin and Baker (1972), Rule et al. (1980), and Perrolle (1983), for treatments of privacy and computers.

21. For example, in 1983 a federal judge in the District of Columbia ruled that a form mailed to 4 million social security recipients "makes a mockery of the consent requirement." The crippled, blind, and disabled recipients of supplemental security income were led to believe that their assistance might be denied if they refused to authorize access to their otherwise confidential tax returns.

22. For example, U.S. Department of Health and Human Services auditors found that the Social Security Administration's system for transferring large volumes of data between centralized computers and local offices could be improperly accessed rather easily. This was also the case for access to Social Security Administration terminals (U.S. Department of Health and Human Services, 1981: 11).

23. For a discussion of the politics of conferring "routine use" status, see Kircher (1981).

24. For example, Office of Management and Budget guidelines for federal matching programs require that information concerning "routine use" matches be published in the *Federal Register* in reasonable proximity to their implementation. Technically, those subject to data searching are given notice in this way. However such publication requirements may have little meaning, since those subject to data searching are unlikely to read the *Federal Register*. Furthermore, "the reasonable proximity" requirement does not assure publication before the search is implemented. For example, a match conducted on federal student loans in August 1982 was not published in the *Federal Register* until December 1982 (U.S. Senate, 1982: 182).

25. What is often the *fait accompli* and incomprehensible and hidden nature of the process for determining guilt may show some parallel to the use of witches and trial by ordeal and other magical means for determining guilt.

26. For example, see U.S. Senate (1982: 4-40).

27. One difficulty in assessing impact is whether or not the rates of infraction stay the same. For example, 1981-1983 saw a significant increase in the use of systematic data searching and a concomitant rise in the discovery of fraud. But it is difficult to know how much of this is due to better discovery and how much to a worsened economy that may have resulted in increased rates of fraud.

28. Undercover means, for example, are expensive, restricted in scope, intrusive, and may "discover" crimes that would not have occurred were it not for the instigative activity of the investigation. Yet they can make discoveries not possible with other means. The investigator can exercise considerable initiative over the process. In contrast, efforts to increase citizen reporting are still relatively passive and dependent on whether or not, and with what, citizens choose to come forward. Undercover means are inexpensive and can cover a broad range of persons and areas. Anonymous means such as hotlines can encourage responsible as well as irresponsible accusations. Systematic data searching can be broad in scope and

450 AMERICAN BEHAVIORAL SCIENTIST

relatively inexpensive, and can avoid problems such as generating crime or maliciously inspired accusations, but, as noted, it has other costs.

29. Of course, keeping it a secret may work against the goal of deterrence. An implicit choice may be made between minimizing neutralization and maximizing deterrence. One solution is to hint at the powerful means of discovery being used without being specific. But leaks and the experience of apprehended persons work against this.

30. Lipsky (1980: 122), for example, finds that the routinization of bureaucratic functions reduces the chance to discover unique circumstances requiring flexible responses. The problem is compounded when a computer rather than a human agent is involved. Reliance on the computer (or any other machine) as a surrogate for human decision making may permit violations that deviate from the average to go undetected.

31. For example, in using a social security number other than one's own the unsophisticated person may simply make up a number and run the risk of being detected because he or she has chosen a number that was never issued. But sophisticated offenders will simply take a genuine number belonging to someone else and use that. Their chance of being discovered via a match of claimed to real social security numbers is slight. On the frequency and ease with which false identification is used, see the Report of the Federal Advisory Committee (1976).

32. This depends on the relative distribution of offender types. There is likely to be significant variation across offenses.

33. Beyond pushing toward discovery of a particular type of offender within an offense category, the computer may subtly influence the type of offenses to which police devote their energies. For example, a former chief of the Kansas City Police Department believes that computerization has led to an undue focus on minor offenses (unregistered cars, parking scofflaws) that can be dealt with very efficiently at the expense of other more important and difficult to solve crime problems (cited in Goldman 1983). The effectiveness of the means becomes an important, and often barely recognized, factor in deciding what ends will be pursued.

REFERENCES

- ALTHEIDE, D. (1975) "The irony of security." *Urban Life* 4: 179-195.
- and J. JOHNSON (1980) *Bureaucratic Propaganda*. Boston: Allyn & Bacon.
- ARSON NEWS (1981) "Arson control has most successful year." January.
- BLACK, D. (1980) *The Manners and Customs of Police*. New York: Academic.
- BURNHAM, D. (1983) *The Rise of the Computer State*. New York: Random House.
- COHEN, S. (1979) "The punitive city: notes on the dispersal of social control." *Contemporary Crises* 3, 4: 339-363.
- FOUCAULT, M. (1977) *Discipline and Punish: The Birth of the Prison*. New York: Pantheon.
- GOLDMAN, D. (1983) "The electronic Rorschach." *Psychology Today* (February): 36-43.

- GREENWOOD, P. (1982) *Selective Incapacitation*. Santa Monica, CA: Rand Corporation.
- KATZ, J. (1978) "Concerted ignorance: the social construction of cover-up." *Urban Life* 8: 295-316.
- KIRCHER, J. (1981) "A history of computer matching in federal government programs." *Computerworld* (December 14).
- KUTTNER, B. (1983) "The declining middle." *Atlantic* (July): 60-72.
- LAUDON, K. C. (1983) "Data quality and due process in large record systems: criminal record systems." *Communications of the Assn. for Computing Machinery*.
- LIPSKY, M. (1980) *Street Level Bureaucrats*. New York: Russell Sage.
- MARX, G. T. (1983) "Notes on the discovery, collection and assessment of hidden and dirty data," in J. Kitsuse and J. Schneider (eds.) *Studies in the Sociology of Social Problems*. Norwood, NJ: Ablex.
- (1982) "Who really gets stung: some questions regarding the new police undercover work." *Crime and Delinquency* 28: 165-193.
- (1981) "Ironies of social control: authorities as contributors to deviance through escalation, nonenforcement and covert facilitation." *Social Problems* 28: 221-246.
- MAWBY, R. I. (1981) "Overcoming the barriers of privacy." *Criminology* 18: 501-521.
- National Legislative Conference on Arson (1982) *Anti-Arson Manual*. Columbus, OH: Author.
- New York Civil Liberties Union (1982) *An Evaluation of New York State's Wage Reporting System: The Real Cost of Computer Matching*. New York: Author.
- PARKER, D. (1976) *Crime by Computer*. New York: Scribner.
- PERROLLE, J. (1983) "Computer generated social problems." Presented at the meeting of the Society for the Study of Social Problems, Detroit.
- President's Council on Integrity and Efficiency (1983) *A Summary Report of Inspectors General's Activities*. Washington, DC: Government Printing Office.
- REICHMAN, N. (1983) "Ferretting out fraud: the manufacture and control of fraudulent insurance claims." Ph.D. dissertation, Massachusetts Institute of Technology.
- REISS, A. (1971) *The Police and the Public*. New Haven, CT: Yale Univ. Press.
- Report of the Federal Advisory Committee on False Identification (1976) *The Criminal Use of False Identification*. Washington, DC: Government Printing Office.
- REUTER, J. and J. RUBENSTEIN (1978) "Fact, fancy and organized crime." *Public Interest*: 45-67.
- RULE, J., D. McADAM, L. STEARNS, and D. UGLOW (1980) *The Politics of Privacy*. New York: New American Library.
- SELZNICK, P. (1948) "Foundations of the theory of organization." *Amer. Soc. Rev.* 13.
- SILBEY, S. and E. BITTNER (1982) "The availability of law." *Law and Policy Q.* 4: 399-434.
- SKOLNICK, J. and J. WOODWORTH (1967) "Bureaucracy, information and social control: a study of a morals detail," pp. 99-136 in D. Bordua (ed.) *The Police*. New York: John Wiley.
- SPITZER, S. (1979) "The rationalization of crime control in capitalist society." *Contemporary Crises* 2, 3: 187-206.

452 AMERICAN BEHAVIORAL SCIENTIST

- STINCHCOMBE, A. (1963)** "Institutions of privacy in the determination of police administrative practice." *Amer. J. of Sociology* 69: 150-160.
- Technology Review (1983)** "When computers track criminals." April: 75-76.
- U.S. Department of Health and Human Services, Office of the Inspector General (1981)** *Annual Report*. Washington, DC: Government Printing Office.
- U.S. General Accounting Office (1982)** *IRS Can Do More to Identify Tax Return Processing Problems and Reduce Processing Costs*. Washington, DC: Government Printing Office.
- U.S. Senate, Committee on Governmental Affairs, Subcommittee on Oversight of Government Management (1982)** *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs*. Washington, DC: Government Printing Office.
- U.S. v. Harrison (1982)** 667 F2d 1158, Fourth Circuit Court of Appeals.
- VAUGHAN, D. (1980)** "Crime between organizations: implications for victimology," pp.77-97 in G. Geis and E. Stotland (eds.) *White Collar Crime: Theory and Research*. Beverly Hills, CA: Sage.
- WESTIN, A. and M. BAKER (1972)** *Databanks in a Free Society: Computers, Record-Keeping and Privacy*. New York: Quadrangle.
- WHITESIDE, T. (1978)** *Computer Capers*. New York: New American Library.



U.S. Department of Justice
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

30 MAR 1984

Honorable Robert W. Kastenmeier, Chairman
Subcommittee on Courts, Civil Liberties,
and the Administration of Justice
Committee on the Judiciary
House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

You recently requested that the Department of Justice provide you with information concerning the prosecution of alleged Selective Service nonregistrants. The information provided below is current to March 18, 1984.

First, you asked how many names the Selective Service System referred to the Department of Justice and requested that such information be broken down by year.

In 1981, the Selective Service made 183 referrals. In 1982, the Service made 292 referrals. In 1983, the Service made three referrals of computer tapes containing information on possible nonregistrants. The first tape contained information concerning 5,151 possible nonregistrants; the second, information concerning 76,529 possible nonregistrants; and the third, information concerning 118,346 possible nonregistrants. 1/

Second, you asked how many of the referred names came from a computer match performed by Selective Service.

The 1983 referrals overwhelmingly resulted from Selective Service's matching of registration records with state departments of motor vehicles records. However, such referrals also contain a relatively small number of names of persons who reported themselves as nonregistrants and of persons who were reported by others.

1/ The information on the tapes cannot be added together to determine the total number of nonregistrants since subsequent tapes contain the identities of possible nonregistrants from former tapes. Similarly, the final tape does not represent the entire universe of referred possible nonregistrants since it excludes previously referred persons who registered, were determined not to be within the registration class, or were previously selected by the Department of Justice for investigation and possible prosecution.

Third, you asked how many nonregistrant matters were referred to United States Attorneys and how many were investigated by the Federal Bureau of Investigation.

We refer nonregistrant matters both to the appropriate United States Attorneys and to Federal Bureau of Investigation Headquarters. The Bureau counts as "investigated" every matter referred, even if the field agent only contacts the United States Attorney. Consequently, the number of nonregistrant matters referred to United States Attorneys and the number "investigated" by the FBI should be identical. Those numbers follow.

<u>YEAR</u>	<u>1981</u>	<u>1982</u>	<u>1983</u>
REFERPALS	151	139	372

Fourth, you asked how many prosecutions have been initiated, how many convictions obtained, how many cases appealed, and what the status is of the cases on appeal.

Sixteen alleged nonregistrants have been indicted. Eight have been convicted (including one guilty plea). One indicted nonregistrant was placed in the pretrial diversion program when he registered. One court struck language from an indictment, and another dismissed an indictment.

The Government appealed the dismissal and the striking of language from the indictment. The Ninth Circuit Court of Appeals reversed the dismissal. The defendant has petitioned the Supreme Court for a writ of certiorari. The Government's appeal of the striking of the language from the indictment is pending in the Eighth Circuit Court of Appeals.

Four defendants have appealed their convictions. The Ninth Circuit Court of Appeals affirmed one conviction, the Sixth Circuit Court of Appeals remanded a case for a hearing on defendant's claim that he was selectively prosecuted, ^{2/} and the appeals to the Eighth and First Circuit Courts of Appeals are still pending.

Fifth, you asked how much money has been expended by the Department in enforcing the nonregistration prohibition and asked that this figure be broken down according to expenditures for record keeping, investigating, and prosecuting.

The only such records kept in a reasonably retrievable manner are kept by the Federal Bureau of Investigation. The Bureau informed us that for FY 1982 it expended \$62,634 in salary

^{2/} The Government petitioned for rehearing and suggested that the rehearing be en banc. The Sixth Circuit Court of Appeals denied the petition. The Government is presently considering whether to petition the Supreme Court for a writ of certiorari.

1004

for agents and support personnel for the purpose of investigating nonregistrant matters; in FY 1983 it expended \$73,509 in salary for agents and support personnel; and in FY 1984 (through February 1, 1984) it expended \$40,495 in salary for agents only.

Of course, we hope the information set out above will be responsive to your inquiry.

Sincerely,

(Signed) **Robert A. McConnell**

Robert A. McConnell
Assistant Attorney General

APPENDIX 4

1984: CIVIL LIBERTIES AND THE NATIONAL SECURITY STATE—JANUARY 24, 1984

APPENDIX I—LEGISLATIVE MATERIALS

1. H.R. 6343, 98th Cong., 2d Sess. (1984).

APPENDIX II—CASES

1. *U.S. v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).
2. *U.S. v. Seidlitz*, 589 F.2d 152 (4th Cir. 1980).
3. *U.S. v. Butenko*, 494 F.2d 593 (3d Cir. 1974).
4. *People v. Teicher*, 52 N.Y.2d 638 (Ct. of Appeals, 1981).
5. *People v. Teicher*, 395 N.Y.S.2d 587 (Sup. Ct. 1977).
6. *State v. Jennings*, 611 P.2d 1050 (Idaho, 1980).
7. *In Re Applications of Roberts Flying Service, Inc.*, F.C.C. Docket No. 18870 (1971).
8. *U.S. v. New York Telephone Co.*, 434 U.S. 159 (1977).
9. *Simmons v. Southwestern Bell Telephone Co.*, 452 F. Supp. 392 (W.D. Okla. 1978).
10. *U.S. v. Hall*, 488 F.2d 193 (1973).
11. *Smith v. Wunker*, 356 F. Supp. 44 (S.D. Ohio 1972).
12. *Jabara v. Webster*, ——— F.2d ——— (6th Cir. 1984).
13. *State of Kansas v. Howard*, ——— Kan. ——— (Kan. Sup. Ct. 1983).
14. *People v. Dexek*, Mich. App., 308 N.W.2d 652 (1981).
15. *Application of Order Authorizing Interception of Oral Communications and Videotape Surveillance*, 513 F. Supp. 421 (1980).
16. *U.S. v. Torres*, ——— F.2d ——— (7th Cir. 1984).
17. *U.S. v. Bowler*, 561 F.2d 1323 (1977).

APPENDIX III—ARTICLES AND MISCELLANEOUS MATERIALS

1. Burnham, "Can Privacy and Computer Coexist?," *New York Times*, November 5, 1983.
2. Brownstein, "Computer Communications Vulnerable as Privacy Laws Lag Behind Technology," 16-2 *Nat'l Journal* 52 (Jan. 14, 1984).
3. *Globe*, "Spy Tech," *Christian Science Monitor* (pts. 1-6) April 16, 17, 18, 19, 20, and 23, 1984.
4. Schrage, "U.S. May Tighten Electronic Net to Control Software," *Washington Post*, May 6, 1984.
5. Burnham, "Reagan Orders Action on Eavesdropping," *N.Y. Times*, Oct. 15, 1984.
6. Serrill, "The No Man's Land of High Tech," *Time*, Jan. 14, 1985.
7. Letter from U.S. Department of Justice, Criminal Division, to Hon. Robert W. Kastenmeier, dated December 27, 1983, with attachments.

APPENDIXES—3

APPENDIX—I

98TH CONGRESS
2D SESSION**H. R. 6343**

To amend title 18 of the United States Code with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 1, 1984

Mr. KASTENMEIER introduced the following bill; which was referred to the Committee on the Judiciary

A BILL

To amend title 18 of the United States Code with respect to the interception of certain communications, other forms of surveillance, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*
3 That this Act may be cited as the "Electronic Surveillance
4 Act of 1984".

5 SEC. 2. (a) Section 2510(4) of title 18 of the United
6 States Code is amended by striking out "aural".

7 (b) Section 2510(11) of title 18 of the United States
8 Code is amended by inserting ", and, in the case of an inter-
9 ception pursuant to an order under this chapter, includes any
10 person with respect to whom the applicant for such order had

1 reasonable cause to believe was involved in the activity being
2 investigated through such interception” after “directed”.

3 SEC. 3. Section 2515 of title 18 of the United States
4 Code is further amended by adding at the end “Whenever
5 the interception of a communication otherwise in accordance
6 with this chapter has failed to meet the minimization require-
7 ment of section 2518(5) of this title, and such failure is part
8 of a pattern of intentional illegality, the court may order that
9 no part of the contents of any communication intercepted
10 during the course of conduct demonstrating that pattern, and
11 no evidence derived therefrom, may be received in any such
12 trial, hearing, or other proceeding, and may also make appro-
13 priate orders preventing the use or disclosure of any such
14 contents.”.

15 SEC. 4. Section 2516(1)(c) of title 18 of the United
16 States Code is amended by inserting “section 1512 (tamper-
17 ing with a witness, victim, or an informant), section 1513
18 (retaliating against a witness, victim, or an informant),” after
19 “(obstruction of State or local law enforcement),”.

20 SEC. 5. Section 2517(5) of title 18 of the United States
21 Code is amended—

22 (1) by striking out “When” and inserting “To the
23 extent” in lieu thereof; and

24 (2) by inserting “solely” after “relating”

1 SEC. 6. (a) Section 2518(1)(b) of title 18 of the United
2 States Code is amended by inserting immediately before the
3 semicolon at the end the following: “, and (v) the specific
4 investigative objectives and the specific targets, of the inter-
5 ception to which the application pertains”.

6 (b) Section 2518(1)(c) of title 18 of the United States
7 Code is amended—

8 (1) by inserting “(including the use of informants,
9 search warrants, interviewing witnesses, and obtaining
10 documents through other legal means)” after “proce-
11 dures”; and

12 (2) by striking out “or why they” and inserting in
13 lieu thereof “and establishing that any further use of
14 such procedures would”.

15 (c) Section 2518(3) of title 18 of the United States Code
16 is amended by inserting “(and outside that jurisdiction in the
17 case of a motile interception device installed within such ju-
18 risdiction)” after “within the territorial jurisdiction of the
19 court in which the judge is sitting”.

20 (d) Section 2518(4) of title 18 of the United States Code
21 is amended by adding at the end “A communication shall not
22 be intercepted under an order under this chapter unless at
23 least one of the parties to such communication is identified in
24 such order, the court issuing such order found probable cause
25 that virtually everyone using the designated facility or tele-

1 phone is doing so for the purpose which is the object of inves-
2 tigation set forth in such order, or for the purpose of monitor-
3 ing to become familiar with the voices of targets set forth in
4 such order. The use or disclosure of information obtained by
5 an interception which is authorized under this chapter and
6 utilizes an automatic listening device shall be treated under
7 this chapter in the same manner as the use and disclosure of
8 information obtained by an interception not using such a
9 device. An order authorizing the interception of a wire or
10 oral communication under this chapter may, upon a showing
11 by the applicant that there are no other less intrusive means
12 of effecting the interception, authorize physical entry to in-
13 stall an electronic, mechanical, or other device.”.

14 (e) Section 2518(5) of title 18 of the United States Code
15 is amended by inserting “with the good faith intent to mini-
16 mize and” before “in such a way as”.

17 (f) Subsection (6) of section 2518 of title 18 of the
18 United States Code is amended to read as follows:

19 “(6) An order authorizing interception pursuant to this
20 chapter shall require that reports be made not less often than
21 fortnightly to the judge who issued such order, showing what
22 progress has been made toward achievement of the author-
23 ized objective, the need, if any for continued interception, and
24 whether any evidence has been discovered through such
25 interception of offenses other than those with respect to

1 which such order was issued. The judge may suspend or ter-
2 minate interception if any such report is deficient, evinces
3 serious procedural irregularities, or indicates the legal basis
4 of continued interception no longer exists.”.

5 (g) Section 2518(7) of title 18 of the United States Code
6 is amended—

7 (1) by inserting “conspiratorial activities of a life-
8 threatening nature,” before “conspiratorial activities”
9 the first place it appears;

10 (2) by inserting a comma after “security interest”;

11 and

12 (3) by inserting “, upon oral notice to a judge of
13 competent jurisdiction,” after “may”.

14 (h) Section 2518(8)(a) of title 18 of the United States
15 Code is amended by striking out “Immediately upon” and
16 inserting “Not later than 48 hours after” in lieu thereof.

17 SEC. 7. (a) Chapter 119 of title 18 of the United States
18 Code is amended by adding at the end the following:

19 “§ 2521. **Pen registers and tracers**

20 “(a) No person acting under the authority of the United
21 States shall install or use any pen register or tracer except as
22 provided in this section.

23 “(b) For the purposes of this chapter, the installation
24 and use of a pen register or a tracer shall be treated as
25 though such installation or use were an installation or use of

1 an electronic, mechanical, or other device for the interception
2 of a wire or oral communication, and a Federal law enforce-
3 ment officer with responsibility for an ongoing criminal inves-
4 tigation may engage in such installation or use to the extent
5 that this chapter allows the installation or use of a device for
6 such an interception.

7 “(c) As used in this section—

8 “(1) the term ‘pen register’ means a device which
9 records or decodes electronic or other impulses which
10 identify the numbers dialed or otherwise transmitted on
11 the telephone line to which such device is attached;
12 and

13 “(2) the term ‘tracer’ means an electronic or me-
14 chanical device which permits the tracking of a person
15 or object without the consent or knowledge of such in-
16 dividual or the individual controlling such object.”.

17 (b) The table of sections at the beginning of chapter 119
18 of title 18 of the United States Code is amended by adding at
19 the end the following new item:

“2521. Pen registers and tracers.”.

20 SEC. 8. (a) Chapter 205 of title 18 of the United States
21 Code is amended by adding at the end the following:

22 “§ 3117. Video surveillance

23 “(a) No person acting under the authority of the United
24 States shall engage in any video surveillance except as pro-
25 vided in this section.

1 “(b) For the purposes of chapter 119 of this title, video
2 surveillance shall be treated as though such surveillance were
3 an interception of a wire or oral communication, and a Feder-
4 al law enforcement officer with responsibility for an ongoing
5 criminal investigation may engage in video surveillance to
6 the extent that such chapter allows such an interception,
7 except that—

8 “(1) an application under that chapter with re-
9 spect to video surveillance may be made only to a Fed-
10 eral judge of competent jurisdiction;

11 “(2) an order authorizing or approving such sur-
12 veillance shall be for a period not greater than ten
13 days, and each extension of such an order shall be for
14 a period not greater than ten days; and

15 “(3) for the purposes of the application of section
16 2518(1)(c) of this title, other investigative procedures
17 include an interception under chapter 119 of this title.

18 “(c) As used in this section, the term ‘video surveillance’
19 means the recording of visual images of individuals by televi-
20 sion, film, videotape, or other similar method, in a location
21 not open to the general public and without the consent of that
22 individual.”.

23 (b) The table of sections for chapter 205 of title 18 of
24 the United States Code is amended by adding at the end the
25 following new item:

“3117. Video surveillance.”.

1 SEC. 9. (a) Section 1806(e) of title 50 of the United
2 States Code is amended by adding at the end “Any person
3 may make a motion to exclude from any criminal proceeding
4 any evidence obtained or derived from an electronic surveil-
5 lance if the primary purpose of the portion of such surveil-
6 lance from which such evidence was obtained or derived was
7 to obtain information to be used in a criminal proceeding. For
8 the purposes of the immediately preceding sentence a portion
9 of electronic surveillance which occurs not more than 30 days
10 before the return of a criminal indictment based on such sur-
11 veillance shall be presumed to be for the primary purpose of
12 obtaining information to be used in a criminal proceeding.

13 (b) Section 1808(b) of title 50 of the United States Code
14 is amended by striking out “On” and all that follows through
15 “four years thereafter” and inserting in lieu thereof “On or
16 before October 25 of each year”.

17 (c) Section 1807 of title 50 of the United States Code is
18 amended—

19 (1) by striking out “and” at the end of paragraph

20 (a);

21 (2) by striking out the period at the end of para-
22 graph (b) and inserting “; and” in lieu thereof; and

23 (3) by adding at the end the following:

24 “(c) the number of individuals, within a range of 10,
25 who have been the objects of electronic surveillance.”.

1 (d) Section 1805(b)(2) of title 50 of the United States
2 Code is amended—

3 (1) by striking out “and” at the end of subpara-
4 graph (C);

5 (2) by striking out the period at the end of sub-
6 paragraph (D) and inserting “; and” in lieu thereof;
7 and

8 (3) by adding at the end the following:

9 “(E) that the applicant inform any United
10 States person whose communication is intercepted
11 by electronic surveillance of the fact of such sur-
12 veillance not later than 180 days after the end of
13 such surveillance, unless the United States estab-
14 lishes to the satisfaction of the court by clear and
15 convincing evidence that so to inform such person
16 would jeopardize an ongoing intelligence operation
17 or disclose the sources or methods of intelligence
18 gathering.”.

19 SEC. 10. This Act and the amendments made by this
20 Act shall take effect 30 days after the date of the enactment
21 of this Act.

UNITED STATES of America, Appellee,

v.

TRUONG DINH HUNG, Appellant.

UNITED STATES of America, Appellee,

v.

Ronald Louis HUMPHREY, Appellant.

Nos. 78-5176, 78-5177.

United States Court of Appeals,
Fourth Circuit.

Argued Dec. 6, 1979.

Decided July 17, 1980.

Defendants were convicted in the United States District Court for the Eastern District of Virginia, Albert V. Bryan, Jr., J., of espionage, conspiracy to commit espionage and several espionage-related offenses for transmitting classified information to representatives of the Socialist Republic of Vietnam during the 1977 Paris negotiations between that country and the United States, and they appealed. The Court of Appeals, Winter, Circuit Judge, held that:

(1) evidence obtained pursuant to reasona-

ble warrantless searches and surveillances of defendants prior to time that investigation became "primarily" criminal investigation was admissible against defendants; however, evidence obtained through warrantless surveillance subsequent to that time was properly excluded; (2) application of statute requiring agents of a foreign government to register did not violate Fifth Amendment; (3) appeals from espionage and espionage-related convictions would be remanded for further proceedings to determine whether documents produced by Government near end of trial contained Jencks Act material that should have been supplied to the defense; and (4) Jencks Act was not violated by destruction of confidential CIA informant's written reports to her superior for reason that the reports, which had been destroyed according to routine CIA procedures before any criminal prosecution was contemplated, were destroyed outside context of a criminal investigation.

Affirmed and remanded.

Donald Russell, Circuit Judge, filed separate opinion in which he concurred in part and dissented in part and in which K. K. Hall, Circuit Judge, joined.

1. Searches and Seizures \S 7(I)

Under foreign intelligence exception to Fourth Amendment, government will be relieved of seeking warrant only in those situations in which interests of the executive are paramount, when object of search or surveillance is a foreign power, its agent or collaborators and only when surveillance is conducted "primarily" for foreign intelligence reasons. U.S.C.A. Const. Amend. 4.

2. Criminal Law \S 394.4(1)

Evidence obtained pursuant to reasonable warrantless searches and surveillances of defendants, employees of United States information agency was furnished copies of classified documents to codefendant who then delivered them to representatives of Socialist Republic of Vietnam during 1977 Paris negotiations between that country and the United States, prior to time that investigation became "primarily" criminal

Cite as 629 F.2d 908 (1980)

that he was a source of the documents sometime during his conversation with Truong. As well, when the government eavesdrops on clandestine groups like this one, investigators often find it necessary to intercept all calls in order to record possible code language or oblique references to the illegal scheme. See *United States v. Clerkley*, 556 F.2d 709 (4 Cir.1977), cert. denied sub nom. *London v. United States*, 436 U.S. 930, 98 S.Ct. 2830, 56 L.Ed.2d 775 (1978) (approving blanket surveillance of numbers operation in order to determine the participants). Thus, on the facts of this case the surveillance conducted by the government agents was reasonable.⁷

C. Package Search

[5] The FBI and the CIA searched one of the packages Truong sent to Paris by Krall without either the authorization of the Attorney General or a search warrant. Because the government agents did not receive executive authorization, the foreign intelligence exception to the warrant requirement does not legitimate this search. Nevertheless, because Truong did not have a legitimate expectation of privacy in the package, see *United States v. Rabinowitz*, 339 U.S. 56, 65-66, 70 S.Ct. 430, 435, 94 L.Ed. 653 (1950), the district court did not err in permitting the contents of the package to be admitted into evidence.

The package of documents was contained within an unsealed manila envelope. Inside the envelope was a transparent bookbag, loosely tied with twine. Although the documents were partially shielded from view by opaque pieces of paper, some parts of the documents could be seen through the bookbag. Thus, Truong had not made a diligent effort to conceal the documents from view.

7. In addition to the surveillance of Truong, the government installed a secret video tape camera in Humphrey's office at the United States Information Agency. In his brief, Humphrey does not discuss this intrusion at length, perhaps because the evidence obtained from the video tape did not play an important role at trial. In any case, we affirm the ruling of the district court that the video-taping was reasonable up to July 20, because the FBI took steps to minimize the intrusion and because the tap-

Moreover, Truong knew that this flimsily wrapped package would cross at least two national boundaries on its way to Paris. This risk of inspection when Krall left the United States and when she entered France militates against any expectation of privacy by Truong. See *United States v. Ramsey*, 431 U.S. 606, 97 S.Ct. 1972, 52 L.Ed.2d 617 (1977). Therefore, because the package was poorly wrapped and because it was destined for foreign delivery, Truong could not have harbored a reasonable expectation that the contents of the package would remain undisclosed; and consequently neither a search warrant nor executive authorization was necessary for this search.⁸

III.

The defendants were convicted of several violations of the espionage statutes and related provisions. Truong and Humphrey raise a number of challenges to these convictions.

A. Espionage Statutes

The jury found that the defendants had violated three espionage provisions, 18 U.S.C. § 794(a), § 794(c), and § 793(e). Two principal objections are made by the defendants to their convictions under these statutes, and we will consider them in order:

(1) National Defense

[6] A common prerequisite for a conviction under each of the statutes is that the defendant transmit information "relating to the national defense." The defendants argue that this phrase limits the reach of the statutes to military matters and assert that none of the materials transmitted by

ing was necessary to determine how Humphrey handled government documents while at work.

8. A letter and another package were searched without a warrant but with executive authorization. Because both of those searches took place before July 20, in accordance with our resolution of the issue of a foreign intelligence warrant exception, we conclude that neither of these warrantless searches violated the Fourth Amendment.

[8] We are mindful of the strict standard of review of jury verdicts on the issue of contributory negligence. However, with knowledge of the precise location and dimensions of the defective pavement, Garr proceeded "not thinking" down the sidewalk. We hold that under Pennsylvania law, Garr was contributorily negligent as a matter of law. The judgment of the district court will be reversed.



UNITED STATES of America, Appellee,
v.

Bertram E. SEIDLITZ, Appellant.
No. 76-2027.

United States Court of Appeals,
Fourth Circuit.

Argued July 19, 1978.

Decided Dec. 5, 1978.

Defendant was convicted in the United States District Court for the District of Maryland, Alexander Harvey, II, J., of two counts of fraud by wire, and he appealed. The Court of Appeals, Field, Senior Circuit Judge, held that: (1) use of telephone tracers and "spy" attachment to computer in order to trace the unauthorized user of information stored in computer system did not constitute invalid electronic surveillance so as to invalidate warrant to search defendant's premises, and (2) there was sufficient evidence from which jury could find that computer system was "property" and that defendant had fraudulent intent in using information in computer system without authorization.

Affirmed.

use the sidewalk rather than the customary route down the roadway:

Q. Was there anything that evening that prevented you from waiting for that car to pass and then step into the driveway and walk down the driveway?

A. Other than the fact I just had other things on my mind. I had to get the gloves. I was getting close to the half hour.

1. Criminal Law ⇌ 394.4(1)

A judicially fashioned rule of exclusion applies where surveillance does not comport with Fourth Amendment requirements. U.S.C.A.Const. Amend. 4.

2. Telecommunications ⇌ 494

Communications Act of 1934 had no bearing on legality of activities involving interception of communications with computer system where such communications took place over commercial telephone circuits. Communications Act of 1934, § 605, 47 U.S.C.A. § 605.

3. Telecommunications ⇌ 494

Telephone traces which did not interfere with or observe the contents of dialogues but merely traced source of communications did not constitute "interceptions" of communications proscribed by Title III of Omnibus Crime Control and Safe Streets Act of 1968. 18 U.S.C.A. § 2510(4).

See publication Words and Phrases for other judicial constructions and definitions.

4. Telecommunications ⇌ 494

Use of "spy" attachment to computer in order to trace location of unauthorized user of information stored in computer system was not prohibited by Title III of Omnibus Crime Control and Safe Streets Act of 1968. 18 U.S.C.A. § 2510(4).

5. Criminal Law ⇌ 394.4(1)

Searches and Seizures ⇌ 7(1)

It is no part of policy underlying Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost in their ability in the apprehension of criminals; Fourth Amendment and the exclusionary rule by which it is enforced come into play only where it appears from all of

Q. Well, isn't it true that if you have a reason for extending beyond the half hour, like gloves, that you wouldn't be docked for that?

A. You wouldn't be docked for anything. App. at 86a.

UNITED STATES v. SEIDLITZ

153

Cite as 589 F.2d 152 (1978)

the circumstances that in a particular case the challenged evidence was obtained as a result of a search conducted by government officers or by private persons acting as agents or instrumentalities of the government. U.S.C.A.Const. Amends. 4, 14.

6. Criminal Law ⇐ 394.4(1)

Activities of telephone company in tracing calls, and activities of owners of computer system in using "spy" attachment in order to trace the unauthorized user of information stored in computer system, were not subject to scrutiny under the exclusionary rule of the Fourth Amendment. U.S.C.A.Const. Amend. 4.

7. Telecommunications ⇐ 363

In prosecution for fraud by wire, there was sufficient evidence from which jury could find that information stored in computer system was "property" and that defendant had fraudulent intent in retrieving information from computer system without authorization. 18 U.S.C.A. § 1343.

8. Criminal Law ⇐ 1028

Absent plain or fundamental error, court need not consider on appeal legal points which were available to the appellant but not pressed for the district court's consideration. Fed.Rules Civ.Proc. rules 12(f), 52, 28 U.S.C.A.

David M. Dorsen, Washington, D. C. (Sachs, Greenebaum & Tayler, Washington, D. C., Beverly Sherman Nash, Washington, D. C., Sachs & Greenebaum, Chevy Chase, Md., on brief), for appellant.

1. The federal wire fraud statute, 18 U.S.C. § 1343, provides:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than \$1,000 or imprisoned not more than five years, or both.

Robert A. Rohrbaugh, Asst. U. S. Atty., Baltimore, Md. (Russell T. Baker, Jr., U. S. Atty., Baltimore, Md., on brief), for appellee.

Before WINTER, Circuit Judge, FIELD, Senior Circuit Judge, and HALL, Circuit Judge.

FIELD, Senior Circuit Judge:

Bertram Seidlitz appeals from his conviction on two counts of fraud by wire in violation of 18 U.S.C. § 1343.¹ As grounds for reversal, he urges that the trial court erred in its denial of a pretrial motion to suppress evidence, and that the prosecution failed to establish certain material elements of the crime. Although advanced in a somewhat novel factual context, we find appellant's contentions to be without merit.

On January 1, 1975, defendant Seidlitz assumed the position of Deputy Project Director for Optimum Systems, Inc. (OSI), a computer service company which was under contract to install, maintain, and operate a computer facility at Rockville, Maryland, for use by the Federal Energy Administration (FEA). Under the arrangement between OSI and FEA, persons working for FEA in various parts of the country could use key boards at communications terminals in their offices to send instructions over telephone circuits to the large computers in Rockville, and the computers' responses would be returned and reflected on a CRT (cathode ray tube) terminal which is a typewriter-like device with a keyboard and display screen similar to a television screen upon which the information is displayed as it is sent and received.² Mr. Seidlitz helped

2. A remote user would dial on an ordinary telephone one of the several unpublished telephone numbers to which OSI subscribed and which were assigned to the computers. He would then connect the telephone to his terminal so that messages could be relayed between the terminal and the computers in the form of signals traveling over the telephone line. Because any of a number of commercially available terminal units could accomplish such a link to the computers, the user, as a security precaution, had to enter on his terminal keyboard a special access code before he would be permitted full use of the system. The code con-

to prepare the software³ which was installed at the Rockville facility as part of the project, and he was also responsible for the security of the central computer system. During his tenure, he had full access to the computers and to a software system known as "WYLBUR" which resided within them.⁴ In June, 1975, Seidlitz resigned this job and returned to work at his own computer firm in Alexandria, Virginia.

William Coakley, a computer specialist employed by FEA, was assigned temporarily to the OSI facility. On December 30, 1975, in an attempt to locate a friend who might be using the OSI system, he had the computer display the initials of everyone who was then using the WYLBUR software. Among the initials displayed by the computer were those of his supervisor, who was standing nearby and who was not using the computer. Suspicious that an unauthorized "intruder" might be using these initials in order to gain access to the system,⁵ Coakley asked Mr. Ewing, an OSI employee, if Ewing could determine what was happening. He also asked Mr. Wack, an OSI supervisor, if he (Wack) could determine whether the mysterious user was at a remote terminal or at one of the terminals within the OSI complex which were directly wired to the computer and did not employ telephone circuits. Ewing instructed the computer to display for him the data it was about to transmit to the possible intruder, and it proved to be a portion of the "source

ained, among other things, the user's personal initials, which were to be invalidated when he left OSI or FEA. This "access code" would be communicated to the central computers which, if they recognized the code as belonging to an authorized user, would proceed to perform the work the individual sent along.

3. To be distinguished from "hardware", which is the tangible machinery of the computer, "software" refers to the logic and directions loaded into the machine that cause it to do certain things on command.

4. The WYLBUR software system facilitated the computers' exchanges with FEA users at the remote terminals. It contained no classified FEA information, but rather enabled the computers to perform tasks assigned to them by FEA personnel. An OSI manual described WYLBUR as "an online interactive text editor

code" of the WYLBUR software system.⁶ Using other data provided by the computer, Wack concluded that the connection was by telephone from outside the complex. At his request, the telephone company manually traced the call to the Alexandria office of the defendant.⁷ Wack was told that the trace was successful, but the telephone company informed him that it could not divulge the results of the trace except in response to a legal subpoena.

The following day, OSI activated a special feature of the WYLBUR system known as the "Milten Spy Function," which automatically recorded, after they had been received by the machinery at Rockville, any requests made of the computer by the intruder. The "spy" also recorded, before they were sent out to the intruder over the telephone lines, the computer's responses to such requests. Mr. Wack again asked the telephone company to trace the line when it was suspected that the unauthorized person, employing the same initials, was using the computer to receive portions of the WYLBUR source code. This manual trace on December 31 led once more to the defendant's office in Virginia, although OSI was not so informed.

Advised by OSI of the events of December 30 and 31, the FBI on January 3, 1976, secured, but did not then execute, a warrant to search the defendant's Alexandria office.⁸ At the FBI's suggestion, the tele-

designed to facilitate the creation of text and to provide a powerful and comfortable tool for changing, correcting, searching and displaying text."

5. See n. 2, *supra*.

6. A source code is a programming language, understandable to humans, in which a computer is given instructions.

7. A manual trace is accomplished without listening in on the line or breaking into the conversation. It entails a physical tracing of the telephone circuitry backward through the various switching points from the equipment which receives the call.

8. The affidavit in support of the application for the warrant related that the intrusions had

UNITED STATES v. SEIDLITZ

155

Cite as 589 F.2d 152 (1978)

phone company conducted two additional manual traces when alerted to incoming calls by OSI, but in each instance the calls were terminated before the traces had progressed beyond the telephone company's office in Lanham, Maryland, which served 10,000 subscribers. The phone company then installed "originating accounting identification equipment" in the Lanham office, the function of which was to automatically and quickly ascertain, without intercepting the contents of any communication, the telephone number of any of the 10,000 area telephones from which any subsequent calls to the OSI computers originated. Two such calls were made on the morning of January 9, and the equipment attributed both of them to a phone at the defendant's Lanham residence. That afternoon, the FBI executed the warrant to search Seidlitz' Alexandria office, seizing, among other items, a copy of the user's guide to the OSI system and some 40 rolls of computer paper upon which were printed the WYLBUR source code.⁹ A warrant was then issued to search the Seidlitz residence in Lanham,¹⁰ where officers found a portable communications terminal which contained a teleprinter for receiving written messages from the computer, as well as a notebook containing information relating to access codes¹¹ previously assigned to authorized users of the OSI computers.

The indictment handed down on February 3, 1976, charged that the defendant had, on December 30 and 31, transmitted tele-

been detected, that OSI had "furnished written release" to receive information regarding the telephone traces of December 30 and 31, and that the telephone company had disclosed to the FBI that the calls originated from the defendant's office. It also stated that, as a result of an investigation of former OSI employees and interviews with OSI personnel, the FBI, prior to the receipt of the trace information, had ascertained Seidlitz' business address and concluded that he was the chief suspect.

9. The information on these printouts was identified at trial as being identical to the information recorded by the "spy" program on December 31.

10. The affidavit in support of the application for this warrant in essence contained the same statements made in the application for the pri-

phone calls in interstate commerce as part of a scheme to defraud OSI of property consisting of information from the computer system.¹² A motion to suppress the evidence seized from the office and the residence was considered at a hearing on April 30,¹³ after which the district judge rendered an oral opinion rejecting the defendant's argument that the searches were invalidated by the use of illegal electronic surveillance to obtain the information contained in the affidavits supporting the warrants. Specifically, the district judge ruled that (1) as to the information obtained by use of the "spy", Section 605 of the Communications Act of 1934, 47 U.S.C. § 605, does not apply, and neither Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510, et seq., nor the Fourth Amendment were violated, since the information was obtained with the consent of a party to the defendant's telephonic communications, and (2) with respect to the tracing of the telephone calls, neither Title III nor the Fourth Amendment are offended when, as in the "pen register" cases, the number of the telephone from which a call is placed is determined by a process which does not entail the interception of the contents of the communication. Over defense objection, much of the challenged evidence was admitted at trial, and the telephone traces, as well as the operation of the "Miltten Spy", were described to the jury. In the face of this evidence, the defendant conceded that he had retrieved the informa-

or warrant. See n. 8, *supra*. In addition, it related that the FBI had been informed that Seidlitz maintained a communications terminal at his home, that the search of the office had not uncovered the terminal, and that the telephone company's trace of the calls that morning indicated that they were made from the defendant's residence.

11. See n. 2, *supra*.

12. A motion for acquittal on a third count of interstate transportation of stolen property was granted during the course of the trial.

13. The evidence presented at the suppression hearing established all the facts which we have summarized above.

tion from the computers, but claimed to have acted only out of concern for the security of the OSI system. In negation of fraudulent intent, Seidlitz testified that he acquired the data with the sole intention of presenting the printouts to OSI officials to prove to them that the steps taken to prevent unauthorized use of the computers were inadequate. Additionally, it was his position at trial that the WYLBUR software was not a trade secret or other property interest of OSI sufficient to qualify as "property" within the meaning of the wire fraud statute. On appeal he renews the "illegal surveillance" claims and also argues that the evidence before the jury was insufficient to establish either his fraudulent intent or that WYLBUR constituted "property."

[1] In considering the surveillance questions, we assume that if, as the defendant contends, either the "spy" activities or the traces were conducted illegally, then the evidence seized at both the office and the residence should have been suppressed, since the affidavits upon which the warrants were issued contained information attributable to the "spy" and the telephone traces which was essential to the finding of probable cause to search.¹⁴ Furthermore, if the statutory or constitutional standards upon which the defendant relies were transgressed, then the jury should not have been informed of the deployment of the "spy" and the traces of the telephone calls.¹⁵

[2] It can safely be said, however, that even if, as the defendant argues, the Milten Spy or the telephone traces resulted in the "interception" of his communications with the computers, these communications were wire or telephone communications since in

14. In ruling on the motion to suppress, the district court also made this assumption. "[T]he question is whether the information * * * was legally or illegally secured. If, of course, it was illegal, then the searches must fall * * *". Appendix, p. 133.

15. Section 605 of the Communications Act has been interpreted to require the exclusion of evidence obtained in violation thereof, *Nardone v. United States*, 302 U.S. 379, 58 S.Ct. 275, 82 L.Ed. 314 (1937), and an express exclusionary rule is contained in Title III of the Omnibus Act

each instance the defendant was exchanging messages with the computers over commercial telephone circuits.¹⁶ For this reason the district court correctly concluded that Section 605 of the Communications Act of 1934, 47 U.S.C. § 605, could have no bearing whatever upon the legality of these activities. While at one time Section 605 did contain standards for determining the legality of the interception of telephone conversations, the statute was amended by Section 803 of Pub.L. 90-351, 82 Stat. 223, in 1968, for the express purpose of excluding from its scope the interception of wire communications and of transferring the regulation of such activity to certain provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. See *United States v. Clegg*, 509 F.2d 605, 611-612 (5 Cir. 1975); *United States v. Falcone*, 505 F.2d 478, 482 (3 Cir. 1974), cert. denied 420 U.S. 955, 95 S.Ct. 1338, 43 L.Ed.2d 432 (1975); S.Rep.No.1097, 90th Cong., 2d Sess. 107 (1968), reprinted in [1968] U.S.Code Cong. & Admin.News, pp. 2112, 2196. Today Section 605 pertains to the interception of only radio communications, and there is no indication that radio communications of any kind were involved in the apprehension and conviction of the defendant. The appropriate inquiry, then, is whether any of the questioned activities amounted to the kind of interceptions of wire communications condemned by Title III.

[3] The language, the legislative history, and the Supreme Court's interpretation of the relevant provisions of Title III support the district court's conclusion that the telephone traces in this case were not the sort of "interceptions" of communications

at 18 U.S.C. § 2515. A judicially-fashioned rule of exclusion applies where surveillance does not comport with Fourth Amendment requirements. *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

16. The same can be said of Mr. Ewing's inquiry of the computer on December 30 by which he ascertained, as did the Milten Spy on the following day, that the intruder was receiving part of the WYLBUR source code.

UNITED STATES v. SEIDLITZ

157

Cite as 589 F.2d 152 (1978)

proscribed by the statute. "Intercept" is defined in 18 U.S.C. § 2510(4) to mean "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device" (emphasis added); "'contents' * * includes any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510(8). The evidence adduced at the suppression hearing conclusively shows that neither the manual traces conducted on December 30 and 31, nor the traces which were achieved by use of the special equipment later installed, entailed interference with or observation of the contents of the defendant's dialogues with the computers. That Congress intended to exempt such procedures from the coverage of the statute is borne out by the Senate Report which accompanied the legislation, and explained that

"[t]he proposed legislation is not designed to prevent the tracing of phone calls * * . The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication."

S.Rep.No.1097, *supra*, at 90; U.S.Code Cong. & Admin.News, *supra*, at 2178. See *Michigan Bell Tel. Co. v. United States*, 565 F.2d 385, 387-389 (6 Cir. 1977). Especially in view of *United States v. New York Telephone Co.*, 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977), which held that "pen registers" (which similarly "overhear" none of the substance of a telephone communication, 434 U.S. at 161, n. 1, 98 S.Ct. at 364, n. 1) do not run afoul of the statute, we perceive no reason to invalidate the telephone traces on statutory grounds.

[4] We also concur in the disposition by the court below of the challenge under Title

17. "The words 'aural acquisition' literally translated mean to come into possession through the sense of hearing (Webster's Third New International Dictionary, 1967 Ed.)." *Smith v. Wunker*, 356 F.Supp. 44, 46 (S.D.Ohio 1972).

III to the information obtained through the use of the Milten Spy. First, the statute proscribes only the "aural" acquisition of the contents of wire communications, 18 U.S.C. § 2510(4), *supra*, and there is no evidence to suggest that the "spy" relied in any fashion upon sounds in retrieving information from the computers in written form. Cf. *United States v. New York Telephone Co.*, *supra*, 434 U.S. at 166-167, 98 S.Ct. 364. We find no merit in the defendant's suggestion that, in the absence of either a statutory definition of the word "aural" or of legislative history to indicate that Congress even considered the relationship of Title III to computer systems, we should ignore the plain meaning of the term "aural"¹⁷ and should hold that, regardless of whether a device detects sound, its ability to interpret the substance of a transmission brings it within the restrictions of the statute. Canons of statutory construction require that we attribute to legislatively undefined words their commonly accepted meaning and that we give effect to what must be presumed to have been the purposeful inclusion in the legislation of a qualifying term such as "aural" which restricts the statute's scope.¹⁸ Second, to the extent that the Milten Spy disclosed, before they were sent out over the telephone lines, the substance of the replies generated by the computer to the intruder's commands, the information was not a "wire communication" at the time of its retrieval, and its disclosure thus did not violate the statute. Under Title III, a "wire communication" is a communication made "in whole or in part" through the facilities of a common carrier, 18 U.S.C. § 2510(1), and the portion of the WYLBUR source code requested by Seidlitz was obtained by the "spy" before it had travelled through such facilities. While arguably this reasoning might not apply to

18. See *Platt v. Union Pacific R.R. Co.*, 99 U.S. 48, 58-59, 25 L.Ed. 424 (1878); *State Water Control Board v. Train*, 559 F.2d 921, 924 n. 20 (4 Cir. 1977). These rules are applicable here because the legislative history indicates neither what Congress meant by "aural" nor why the word was written into the statute.

the spy's duplication, after they had been received by the computer, of any of the instructions Seidlitz sent by telephone, it unquestionably legitimizes under the statute that portion of the retrievals which identified the outgoing information as the WYLBUR source code. Finally, Title III specifically authorizes the interception of a wire communication by a party to the communication or by a person acting with the consent of a party to the communication. 18 U.S.C. § 2511(2)(c), (d). In our opinion OSI, which leased, housed, programmed, and maintained the computers and subscribed to the relevant telephone numbers, was for all intents and purposes a party to the communications initiated by the defendant, since in a very real sense the company used the computers solely as a medium for imparting to customers, via telephone lines, its own expertise. Insofar as OSI installed on its line a computer which was capable of recording the messages exchanged in the course of responding to a remote user's requests, we consider this case analogous to those which recognize that a party may, consistent with Title III, use a device to capture and record both sides of his telephone conversation with another party. See, e. g., *United States v. Turk*, 526 F.2d 654 (5 Cir. 1976), cert. denied, 429 U.S. 823, 97 S.Ct. 74, 50 L.Ed.2d 84 (1976); *Smith v. Cincinnati Post & Times-Star*, 475 F.2d 740 (6 Cir. 1973); *Smith v. Wunker*, 356 F.Supp.

19. The three reasons set forth in this paragraph also apply to Mr. Ewing's actions of December 30. See n. 16, *supra*.

20. Interceptions of two-party conversations were discussed in the context of the Fourth Amendment in the cases cited by the district court to support its conclusion. In each instance, government law enforcement officers had arranged and actively participated in the challenged surveillance. See *United States v. White*, 401 U.S. 745, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971); *United States v. Bernstein*, 509 F.2d 996 (4 Cir. 1975); *United States v. Dowdy*, 479 F.2d 213 (4 Cir. 1973). *White* and *Dowdy* do support the view that the voluntary participation in such surveillance by one of the parties to a telephone call will satisfy the Fourth Amendment, and as already indicated, we tend to agree that even if Seidlitz' data transmissions were made with a legitimate expecta-

44 (S.D. Ohio 1972). Cf. *United States v. Bragan*, 499 F.2d 1376 (4 Cir. 1974).¹⁹

[5, 6] The last of the objections raised in the court below to the evidence secured by the Milten Spy and the telephone traces was that it was detected and obtained in contravention of the Fourth Amendment. The district judge rejected this contention on the ground that even though the "spy" and the traces were utilized without prior judicial authorization, the evidence was obtained by searches to which the appropriate persons had consented. We need not review the soundness of that ruling or the implicit conclusion that the "spy" and the traces raised questions under the Fourth Amendment,²⁰ since in our opinion the activities complained of were, at most, conducted by private persons—OSI and the telephone company—to which the constitutional prohibition against warrantless searches does not apply. "[I]t is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals," and consequently the Fourth Amendment and the exclusionary rule by which it is enforced come into play only where it appears from all of the circumstances that in a particular case the challenged evidence was obtained as a result of a search conducted by government officers or by private persons acting as agents or instrumentalities of the

of privacy (a question we do not decide and about which we have serious reservations), the fact that OSI voluntarily recorded them obviates Fourth Amendment concerns as to the "spy". But we are not sure that a similar approach is valid with respect to the traces of the telephone numbers, and the parties have not briefed this aspect of the constitutional issue. Rather than decide either the "open" question of whether the Fourth Amendment applies to such traces, see *United States v. New York Tel. Co.*, *supra*, 434 U.S. at 163, n. 7, 98 S.Ct. 364, n. 7, or the more perplexing question of whether the recipient of a call can, under the Fourth Amendment, consent to a warrantless trace of the caller's telephone, we choose to rest our opinion as to the constitutionality of the "spy" and the traces on the ground set forth in the text.

UNITED STATES v. SEIDLITZ

159

Cite as 589 F.2d 152 (1978)

government. *Coolidge v. New Hampshire*, 403 U.S. 443, 487-490, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). See also *Burdeau v. McDowell*, 256 U.S. 465, 475-476, 41 S.Ct. 574, 65 L.Ed. 1048 (1921); *United States v. Mekjian*, 505 F.2d 1320 (5 Cir. 1975); *United States v. Pryba*, 163 U.S.App.D.C. 389, 592 F.2d 391 (1974), cert. denied, 419 U.S. 1127, 95 S.Ct. 815, 42 L.Ed.2d 828 (1975); *Corngold v. United States*, 367 F.2d 1 (9 Cir. 1966) (en banc). Cf. *United States v. Crabtree*, 545 F.2d 884 (4 Cir. 1976). Emphasizing that FEA's Mr. Coakley, upon discovering the suspicious initials, asked OSI's Ewing "if there was some way that he could determine what this account was doing,"²¹ and that he asked OSI's Wack "if he could determine where the call was coming from,"²² the defendant would have us find that the subsequent determination by OSI that the intruder was receiving the WYLBUR source code, as well as the telephone company's identification of the originating phone numbers, were actions for which the government should be held accountable and to which the Fourth Amendment applies. In our opinion, however, these nonspecific, innocuous remarks by a civilian employee of the FEA were in stark contrast to the active involvement by a Secret Service agent which tainted the search in *Lustig v. United*

States, 338 U.S. 74, 69 S.Ct. 1372, 93 L.Ed. 1819 (1949), cited by the defendant,²³ and they do not amount to the kind of conduct on the part of the government which has been held sufficient to deprive a citizen's search of its private character.²⁴ Under the criteria uniformly considered by the courts in assessing the degree of federal involvement in an otherwise private search for purposes of the Fourth Amendment, the instant "searches" and their fruits are not subject to scrutiny under the exclusionary rule.²⁵

While we base our affirmance of the denial of the suppression motion upon our consideration of the statutory and constitutional arguments advanced by the appellant, and addressed by the court below, we think it appropriate to observe that we discern a certain speciousness which infects all of the illegal surveillance contentions made by the defendant with respect to the evidence which was obtained through use of the Milten Spy. Unlike the typical telephone user who employs the telephone merely as a convenience to converse with other persons over distances, Seidlitz used the telephone to tamper with and manipulate a machine which was owned by others, located on their premises, and obviously not intended for his use. Unlike the party to a

21. Appendix, p. 41.

22. Appendix, p. 42.

23. *Lustig* presented the related question of whether, under the now defunct "silver platter" doctrine, a federal officer was so involved in an illegal search by city police as to require the suppression in a federal prosecution of the evidence uncovered by the search. The facts reveal that a federal Secret Service agent, who was charged with enforcing the counterfeiting laws, joined the unlawful search of a hotel room by city police after it had already begun. While there, he sifted through the items uncovered by the local officers (who were aware of his interest in the case), selecting those articles which were later used as evidence in a federal counterfeiting prosecution of one of the occupants of the room. The Court found that the agent "had an active hand" in the search, and held that the trial court should have suppressed the evidence obtained by him.

24. See the cases collected in Annot., 36 A.L.R.3d 553 (1971).

25. The test most frequently employed is borrowed from the *Lustig* case, supra, 338 U.S. at 79, 69 S.Ct. at 1374, which recognized that "the decisive factor . . . is the actuality of a share by a federal official in the total enterprise of securing and selecting evidence by other than sanctioned means." See also *United States v. Sherwin*, 539 F.2d 1, 7-8 (9 Cir. 1976); *United States v. Entringer*, 532 F.2d 634, 637 (8 Cir. 1976), cert. denied, 429 U.S. 820, 97 S.Ct. 67, 50 L.Ed.2d 81 (1976); *United States v. Clegg*, 509 F.2d 605, 609-611 (5 Cir. 1975); *United States v. Cangiano*, 464 F.2d 320, 324-325 (2 Cir. 1972), vacated and remanded on other grounds, 413 U.S. 913, 93 S.Ct. 3047, 37 L.Ed.2d 1023 (1973), on remand, 491 F.2d 905 (1973), cert. denied, 418 U.S. 934, 94 S.Ct. 3223, 41 L.Ed.2d 1171 (1973); *United States v. Johnson*, 451 F.2d 1321, 1322 (4 Cir. 1971), cert. denied, 405 U.S. 1018, 92 S.Ct. 1298, 31 L.Ed.2d 480 (1972).

personal telephone call who may have little reason to suspect that his words are being covertly recorded, Seidlitz, a computer expert, undoubtedly was aware that by their very nature the computers would record the data he sent and received, and that OSI, also expert in the use of computers, could detect such exchanges if alerted to the presence of an intruder. In this sense the use by the witnesses below of the term "intruder" to describe an unauthorized user of the computers is aptly applied to the defendant, since by telephonic signal he in fact intruded or trespassed upon the physical property of OSI as effectively as if he had broken into the Rockville facility and instructed the computers from one of the terminals directly wired to the machines. Under these circumstances, having been "caught with his hand in the cookie jar", we seriously doubt that he is entitled to raise either statutory or constitutional objections to the evidence.

[7] We have carefully reviewed the other issues raised by the appellant and find them to be without merit. Viewed in the light most favorable to the government, *Glasser v. United States*, 315 U.S. 60, 62 S.Ct. 457, 86 L.Ed. 680 (1942), there was sufficient evidence from which the jury could find that the WYLBUR system was "property" as defined in the instruction given by the trial judge which is not contested on appeal. Even though software systems similar to OSI's WYLBUR were in use at non-OSI facilities, the evidence that OSI invested substantial sums to modify the system to suit its peculiar needs, that OSI enjoyed a multi-million dollar competitive advantage because of WYLBUR, and that OSI took steps to prevent persons other than clients and employees from using the system permitted a finding that the pilfered data was the property of OSI and not, as the defendant contends, property in the public domain subject to appropriation by persons such as himself. In a similar vein, the defendant disputes the sufficiency of the evidence to establish fraudulent intent,

but in essence his argument is only that he feels the jury should not have discredited his own explanation of the purpose for which he acquired the WYLBUR data. It is of no consequence that Seidlitz was not shown by the government to have used the data retrieved from the OSI computers in his own business or to have attempted to sell it to others, see *United States v. Painter*, 314 F.2d 939 (4 Cir. 1963), cert. denied, 374 U.S. 831, 83 S.Ct. 1873, 10 L.Ed.2d 1054 (1963); *United States v. Bagdasian*, 291 F.2d 163 (4 Cir. 1961), cert. denied, 368 U.S. 834, 82 S.Ct. 60, 7 L.Ed.2d 36 (1961), and the circumstantial evidence in this case is ample to support a finding of the requisite intent.

[8] On appeal, the defendant raises other objections relative to the searches of his office and residence, but these points were neither fairly raised in the motion to suppress evidence nor urged upon the trial court at the suppression hearing. Absent plain or fundamental error, we need not consider on appeal legal points which were available to the appellant but not presented for the district court's consideration. *United States v. Braunig*, 553 F.2d 777, 780 (2 Cir. 1977), cert. denied, 431 U.S. 959, 97 S.Ct. 2686, 53 L.Ed.2d 277 (1977); *United States v. Rollins*, 522 F.2d 160, 165-166 (2 Cir. 1975), cert. denied, 424 U.S. 918, 96 S.Ct. 1122, 47 L.Ed.2d 324 (1976); *United States v. Anderson*, 481 F.2d 685, 694-695 (4 Cir. 1973), aff'd, 417 U.S. 211, 94 S.Ct. 2253, 41 L.Ed.2d 20 (1974). See Rules 12(f) and 52, Federal Rules of Criminal Procedure.

AFFIRMED.



UNITED STATES v. BUTENKO

593

Cite as 494 F.2d 593 (1974)

hearing. We conclude that the denial of its requests for discovery resulted in no actual prejudice to Rex.

III.

[6] Rex claims that the evidence does not support the Board's findings that it violated Section 8(a)(1). We disagree.

At the hearing, former employee Garrard testified that on January 27, while Plant Manager Ballard was present, Supervisor Greening asked him if anyone had approached him in the building about union activities, and that Ballard had then commented that employee Wade might approach him about the Union. Garrard further stated that on January 28 Greening asked him if he had overheard any more names of ladies involved in union activities or where union meetings were being held, and said that Rex would be faithful to employees who were faithful to Rex. Finally, Garrard testified that on January 31 Greening asked him if he would sign an affidavit that Wade had approached him in the building about union activities. Employee Poole testified that on January 27, Greening asked her what she had learned at the union meeting the night before, and what the union man had said about transfers of employees within the plant. Although Ballard and Greening contradicted the testimony of Garrard and Poole, the Administrative Law Judge credited the testimony of Garrard and Poole over that of Ballard and Greening where there were conflicts, and found that the interrogations were coercive. Such resolutions of the conflicts in testimony were not unreasonable, and were accepted by the Board. Under these circumstances, it is not our function to overturn them. *NLRB v. Varo, Inc.*, 5 Cir. 1970, 425 F.2d 293, 297-298. Accepting as true the testimony of Garrard and Poole, there was sufficient evidence to support the Board's findings.

4. From the testimony of witnesses, and after his own view of the parking lots and motel, the Administrative Law Judge concluded that

On the issue of surveillance, the General Counsel introduced evidence that on January 27 Supervisor Greening and her husband sat in their car for at least twenty minutes at a store parking lot across the highway from a motel room where the Union was holding a meeting. Several employees testified that while at the meeting they could discern the Greenings in their car. On January 28, Plant Manager Ballard parked his pickup truck in a lot across from the motel and was observed sitting in the truck by employees attending a union meeting at the motel room.⁴ Although the Greenings and Ballard testified that they were not engaged in surveillance, there was sufficient evidence to support a finding of surveillance. See *NLRB v. Standard Forge & Axle Co.*, 5 Cir. 1969, 420 F.2d 508 and cases cited therein.

For the reasons stated, the Board's order is

Enforced.



UNITED STATES of America

v.

John William BUTENKO and
Igor A. Ivanov.

Appeal of Igor A. IVANOV.

No. 72-1741.

United States Court of Appeals,
Third Circuit.

Argued March 20, 1973.

Reargued en banc Nov. 15, 1973.

Decided March 5, 1974.

As Amended April 9, 1974.

Defendant was convicted in the United States District Court for the District of New Jersey of conspiring to

each supervisor parked where he could see the room and recognize employees as they entered.

transmit to foreign government information relating to national defense of United States. The Court of Appeals for the Third Circuit, 384 F.2d 554, affirmed all except one conviction and certiorari was granted. On motion to modify order of remand on writs of certiorari the Supreme Court of the United States, 394 U.S. 165, 89 S.Ct. 961, 22 L.Ed.2d 176, vacated judgment and remanded case. The United States District Court for the District of New Jersey, Anthony T. Augelli, J., 318 F.Supp. 66, denied application for disclosure of communications and the defendant appealed. The Court of Appeals, Adams, Circuit Judge, held, inter alia, that there was presidential power to engage in warrantless surveillance to gather foreign intelligence information, that the overhearing of conversations by defendant during surveillance conducted and maintained solely for purpose of gathering foreign intelligence information did not violate defendant's Fourth Amendment rights and that the court did not abuse its discretion in refusing to order disclosure of records of such interceptions or to hold a hearing regarding them.

Affirmed.

Seitz, Chief Judge, filed a concurring and dissenting opinion in which Van Dusen, Circuit Judge, joined and Aldisert, Circuit Judge, joined in part, Aldisert, Circuit Judge, filed a concurring and dissenting opinion in which Van Dusen, Circuit Judge, joined, and Gibbons, Circuit Judge, filed a dissenting in part opinion.

1. Criminal Law ⇨627.6(6)

Necessity of Government's disclosure to defense of records of electronic surveillance, in cases not involving illegal surveillance, depends on likelihood that accurate determinations of particular factual or legal issues in dispute are otherwise unobtainable.

2. Criminal Law ⇨627.6(6)

Apart from ascertaining whether evidence derived from illegal surveil-

lances tainted a conviction, it remains within trial judge's discretion to require or not to require disclosure of records of surveillances to facilitate resolution of questions surrounding electronic surveillance.

3. Telecommunications ⇨493

Statute relating to prohibition against unauthorized interception of any communication and the divulging thereof prohibits divulgence of intercepted communications obtained by electronic surveillances that are deemed within the parameters of provision. Communications Act of 1934, § 605, 47 U.S.C.A. § 605.

4. Telecommunications ⇨494, 495

Statute prohibiting persons from unauthorized interception and divulgence of communications extends to all of divulgences to any person of any surveillance within provision's ambit. U.S.C.A.Const. Amend. 4; Communications Act of 1934, § 605, 47 U.S.C.A. § 605.

5. Telecommunications ⇨495

Where electronic surveillances were conducted and maintained solely for purpose of gathering foreign intelligence information by Government, Communications Act generally prohibiting the unauthorized interception and divulgence of electronic communication does not render them, in and of themselves, accompanied by subsequent disclosure, unlawful. Communications Act of 1934, § 605, 47 U.S.C.A. § 605; U.S.C.A.Const. art. 2, § 2.

6. Searches and Seizures ⇨7(1)

President, through his subordinates, cannot ignore admonitions of Fourth Amendment when investigating criminal activity unrelated to foreign affairs. U.S.C.A.Const. Amend. 4.

7. Searches and Seizures ⇨7(1)

Fourth Amendment is applicable where President is acting pursuant to foreign affairs duties even though object of surveillance is not a domestic political organization. U.S.C.A.Const. Amend. 4.

UNITED STATES v. BUTENKO

595

Cite as 494 F.2d 503 (1974)

8. Searches and Seizures ⇨7(1)

Under Fourth Amendment all searches and seizures, even if authorized by warrant, must be reasonable which at a minimum means that some form of probable cause for search and seizure must exist and even a reasonable search may be unlawful if official fails to secure a warrant and makes no showing that exigencies of situation make that course imperative.

9. Telecommunications ⇨496

Since the electronic surveillance by Government was conducted and maintained solely for purpose of gathering foreign intelligence information, prior judicial authorization of such surveillance was not required. Communications Act of 1934, § 605, 47 U.S.C.A. § 605; U.S.C.A.Const. Amend. 4.

10. Searches and Seizures ⇨7(1)

Foundation of any determination of reasonableness, which is the crucial test of legality under the Fourth Amendment, is the probable cause standard. U.S.C.A.Const. Amend. 4.

11. Searches and Seizures ⇨7(1)

Search based on probable cause does not comport with Fourth Amendment if its scope is unreasonably broad. U.S.C.A.Const. Amend. 4.

12. Telecommunications ⇨496

Since primary purposes of searches by means of electronic surveillance undertaken to acquire foreign intelligence information is to secure such information, judge, when reviewing particular search, must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental if the warrantless surveillance is to be upheld. U.S.C.A.Const. Amend. 4.

13. Searches and Seizures ⇨7(1)

Since it was found that the second set of interceptions of conversations of defendant, found guilty of conspiring to transmit to foreign government information relating to national defense of the United States, were conducted solely for the purpose of gathering foreign in-

telligence information, the warrantless interceptions, of defendant's conversations were reasonable under Fourth Amendment and the Fourth Amendment rights of defendant were not violated. Communications Act of 1934, § 605, 47 U.S.C.A. § 605; U.S.C.A.Const. Amend. 4.

14. Criminal Law ⇨627.6(1)

Since question confronting trial court as to second set of intercepted conversations of defendant was the legality of the taps and not the existence of tainted evidence, it was within discretion of court to grant or deny defendant's request for a disclosure and the holding of a hearing and exercise of discretion were to be guided by an evaluation of complexity of factors to be considered by court and by likelihood that adversary presentation would substantially promote a more accurate decision. Communications Act of 1934, § 605, 47 U.S.C.A. § 605; U.S.C.A.Const. Amend. 4.

15. Criminal Law ⇨627.6(6)

Where defendant, convicted of conspiring to transmit to foreign government information relating to national defense of United States, did not challenge finding of district court that with respect to the second set of intercepted conversations the surveillance was conducted and maintained solely for purpose of gathering foreign intelligence information, court's failure to order disclosure of records and to hold hearing regarding them did not constitute an abuse of discretion. U.S.C.A.Const. Amend. 4; Communications Act of 1934, § 605, 47 U.S.C.A. § 605.

Jonathan L. Goldstein, John J. Barry, Edward J. Dauber, Asst. U. S. Attys., Newark, N. J., A. William Olson, Asst. Atty. Gen., Robert Keuch, Internal Security Div., Dept. of Justice, Washington, D. C., Herbert J. Stern, U. S. Atty., for appellee.

Edward Bennett Williams, Vincent J. Fuller, Robert L. Weinberg, Williams, Connolly & Califano, Washington, D. C., for appellant.

[1,2] The Supreme Court made clear in *Taglianetti v. United States*¹⁰ that the necessity of disclosure, in cases not involving illegal surveillance, depended upon the likelihood that accurate determinations of the particular factual or legal issues in dispute were otherwise unobtainable. "Nothing in [*Alderman, Ivanov, and Butenko*] . . . requires an adversary proceeding and full disclosure for resolution of every issue raised by an electronic surveillance."¹¹ (Emphasis added) Apart from ascertaining whether evidence derived from illegal surveillances tainted a conviction, it remains within the trial judge's discretion to require or not to require disclosure of records of surveillances to facilitate resolution of questions surrounding electronic surveillance.¹²

Thus, if we are to require disclosure of the records of the second set of interceptions, we must conclude either (1) that the electronic surveillances producing such records were illegal or (2) that the trial judge abused his discretion in refusing disclosure.

In dealing with the former considerations—assessing the legality of the government's activities with regard to the second group of surveillances, we must first decide whether § 605 prohibits the surveillances at issue. If we should decide that the prohibitions of § 605 do not cover these surveillances, we must then proceed to determine whether *Ivanov's* Fourth Amendment rights have been transgressed.¹³ Lastly, if we should hold that this set of surveillances

were not illegal, we must, in accordance with the instructions of the Supreme Court, evaluate the trial judge's exercise of discretion in refusing disclosure.

We shall address these three issues *seriatim*.

II. SECTION 605 OF THE COMMUNICATIONS ACT OF 1934 DOES NOT PROHIBIT THE INTERCEPTION AND DIVULGENCE OF THE CONTENTS OF ELECTRONIC SURVEILLANCE IN THE FOREIGN AFFAIRS FIELD MADE PURSUANT TO EXECUTIVE ORDER.

Section 605 of the Communications Act provides in relevant part that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."¹⁴

This section prompted considerable discussion as electronic surveillance became a more sophisticated and widely used device for the investigation of criminal activity. Much of the clamor for reform centered around the scope given to the section by the *Nardone* cases.¹⁵ Petitioners in those cases were tried and convicted of smuggling alcohol. Over their objection, federal agents were permitted to testify to the substance of petitioners' telephone conversations that were wiretapped and overheard by the witnesses. In *Nardone I*, the Supreme Court held that, under §

10. 394 U.S. 316, 89 S.Ct. 1099, 22 L.Ed.2d 302 (1969) (per curiam).

11. *Id.* at 317, 89 S.Ct. at 1100.

12. Note, The Supreme Court, 1968 Term, 83 Harv.L.Rev. 60, 175 (1969).

13. *Ivanov* contends that the Solicitor General conceded at oral argument before the Supreme Court in *Alderman* that the second set of interceptions were unconstitutional. See *Giordano v. United States*, 394 U.S. 310, 313-314 n. 1, 89 S.Ct. 1163, 22 L.Ed.2d 297 (Stewart, J., concurring). Assuming *arguendo* that *Ivanov* is correct in this regard, it appears that the Supreme Court refused

to accept any such concession and, instead, ordered the district court on remand to consider the question of the legality of these surveillances. *Alderman v. United States*, 394 U.S. 165, 186, 89 S.Ct. 961, 22 L.Ed.2d 176 (1969). See *United States v. Butenko*, 318 F.Supp. 66, 69 (D.N.J.1970).

14. 47 U.S.C. § 605.

15. *Nardone v. United States*, 302 U.S. 379, 58 S.Ct. 275, 82 L.Ed. 314 (1937) [*Nardone I*]; *Nardone v. United States*, 308 U.S. 338, 60 S.Ct. 286, 84 L.Ed. 307 (1939) [*Nardone II*].

UNITED STATES v. BUTENKO

599

CITE AS 494 F.2d 593 (1974)

§ 605. "no person' comprehends federal agents, and the bar on communication to any person' bars testimony to the content of an intercepted message." 16 On re-trial, the prosecution attempted to present evidence gathered as a result of the illegal taps instead of testimony as to the actual contents of the overheard conversations. The Court, in *Nardone II*, made clear that the "fruits" of the taps, as well as the intercepted materials themselves, were inadmissible.

In response to the ostensible debilitating threat to federal investigatory activities presented by the interpretation placed on § 605 by the *Nardone* cases, the Department of Justice adopted the position "that the mere interception of telephone communications is not prohibited by federal law." 17 The government, therefore, continued to wiretap after the *Nardone* cases even though aware that those cases, at least when the surveillances were conducted during the course of an investigation of domestic criminal activity, precluded the introduction of the records or fruits thereof into evidence. Meanwhile, the Department of Justice pressed for legislation lifting the evidentiary limitations erected on the foundation of § 605 by the *Nardone* cases. It did so on the obvious ground that the ability to use electronic surveillance to secure evidence in criminal convictions would make surveillance a more effective weapon against crime. The Department's efforts were finally successful with the enactment of the Omnibus Crime Control and Safe Streets Act of 1968, which specifically authorizes any

electronic surveillance with prior judicial authorization.18 To contend, as Judge Aldisert does, that these efforts by various Attorneys General, constituted a concession that § 605 proscribed the introduction into evidence of material seized as a result of such surveillance does not seem realistic.19 The Attorneys General were advocating new legislation narrowing the potential ambit of § 605 and, in that context, suggesting that § 605 might be broad enough to reach situations like that presented in this case, no doubt represented sound strategy. In addition, the Supreme Court, in the *Nardone* cases, was dealing with the warrantless electronic surveillance of suspected domestic criminals during routine investigations by federal agents. In the present case, we are faced with the significantly different situation of warrantless electronic surveillance pursuant to presidential directive in the sensitive area of foreign intelligence information gathering. It, therefore, would not seem appropriate to regard those cases as controlling here. Only one court of appeals has been faced with circumstances similar to those here and it dealt with the issue obliquely, if at all.20 The Executive Branch's continuing assertion of the power to wiretap per se and the conclusion that the use of intercepted material as evidence was prohibited by § 605 21 and, thus, that the provision had an incidental effect not unlike a rule of evidence, does not, as Judge Aldisert urges, inexorably lead to the proposition that the statutory proscription against divulgence represented an evidentiary rule.22 The legislative

16. 302 U.S. at 381, 58 S.Ct. at 276.

17. Rogers, *The Case for Wire Tapping*, 63 Yale L.J. 792, 793 (1954); Brownell, *Public Security and Wire Tapping*, 39 Cornell L.Q. 193, 197-98 (1954).

18. 18 U.S.C. §§ 2510-2520.

19. During the period covered by the law review articles referred to in Judge Plusert's dissent, electronic surveillances in the field of foreign affairs were made without prior warrants. Indeed, in the instant case, the surveillances were made during the time the

late Robert Kennedy was the Attorney General.

20. See p. 605 *infra*.

21. See, e.g., *Sablowsky v. United States*, 101 F.2d 183 (3d Cir. 1938).

22. Cf. *Developments in the Law—The National Security Interest and Civil Liberties*, 85 Harv.L.Rev. 1130, 1249 (1972). But see *Sablowsky v. United States*, 101 F.2d 183, 189 (3d Cir. 1938) where Judge Biggs stated that "the *Nardone* Case holds clearly that Section 605 creates a rule of evidence."

history relating to § 605 is bereft of any suggestion that Congress intended to fashion a rule of evidence. On the contrary, the language of the statute seems to reach *any* divulgence, by the way of introduction into evidence *or otherwise*, of information obtained by way of wiretaps that would compromise the privacy of those whose conversations are overheard. Furthermore, the fact that the restrictions contained in § 605 have been enforced through the exclusion of evidence at a criminal trial should not obscure the broader aim of the statute—the discouragement of the interception of communications.²³

[3] Thus, in our view, and apparently that of Judge Gibbons, who today dissents on other grounds, § 605 would appear to prohibit divulgence of intercepted communications obtained by electronic surveillances that are deemed within the parameters of the provision. Moreover, restricting any divulgence to members of the Executive Branch, as Judge Aldisert suggests, does not neces-

sarily mean that the surveillance and such divulgence does not run afoul of § 605.²⁴ The proscriptions of § 605 are directed to surveillances generally, and the conjunction, “and,” separating “interception” and “divulgence,” does not seem intended to invite separate analysis. There is absolutely no indication that Congress contemplated situations where interceptions were unaccompanied by divulgences.

[4] However, the conclusion that § 605 extends to all divulgences to any person of any surveillances within the provision's ambit does not exhaust our inquiry into the lawfulness of the wiretaps in the case at hand. We still must determine whether § 605 reaches the type of surveillances producing the records that the district judge has refused to order disclosed to Ivanov and his counsel. Specifically, the question left unanswered is whether § 605 is to be construed to restrict the President's authority to gather foreign intelligence information and use such information to assist in securing criminal convictions.²⁵

23. If, for example, a civil suit were brought by a participant in the conversation, against persons who illegally overheard a conversation, the purpose of the statute—to deter surveillance—would be furthered by some disclosure, at least to the extent such disclosure is necessary to establish the claimed unlawful interception. Cf. *Bivens v. Six Unknown Named Agents of FBI*, 403 U.S. 388, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971).

24. It might be contended, if the “any person” language of the statute were construed liberally, that a divulgence solely within the Executive Branch would not violate § 605. This construction of § 605 would seem to divide the permissible from the impermissible channels of communication for intercepted material along lines not susceptible to explanation in terms of effective governmental response to potentially unlawful activity or in terms of the privacy interests implicated by the statute. Under this interpretation, for example, the Attorney General could openly transmit the contents of intercepted messages through the labyrinthine federal bureaucracy with the attendant risk of substantial invasion of privacy unfettered by even the hortatory effects of § 605, while a discreet revelation of the same material to an officer of a state to aid the latter in ful-

filling his law enforcement duties would be proscribed.

25. With the passage of the Omnibus Crime Control and Safe Streets Act of 1968, it appears that the only limitations on the President's authority to engage in some forms of electronic surveillance are those set forth in the Constitution. Section 2511(3) provides as follows:

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any

UNITED STATES v. BUTENKO

601

Cite as 494 F.2d 503 (1974)

Keeping in mind that § 605 embodies a limitation on the power to engage in surveillance generally, we begin our analysis of the remaining question under the statute with the proposition that the President is charged with the duties to act as Commander-in-Chief of the Armed Forces²⁶ and to administer the nation's foreign affairs,²⁷ powers that should receive fuller treatment in subsequent portions of this opinion.²⁸ To fulfill these responsibilities, the President must exercise an informed judgment on decisions affecting the United States' relationships with other sovereign states and more likely to advance our national interests if the President is apprised of the intentions, capabilities and possible responses of other countries. Certainly one means of acquiring information of this sort is through electronic surveillance. And electronic surveillance may well be a competent tool for impeding the flow of sensitive information from the United States to other nations.

In enacting § 605, the Congress did not address the statute's possible bearing on the President's constitutional duties as Commander-in-Chief and as administrator of the nation's foreign affairs. The Senate and House reports suggest that the purpose of the Communications Act was to create a commission with regulatory power over all forms of electrical communications, whether by telephone, telegraph, cable or radio.²⁹ There appears to have been little or no discussion at all in Congress regarding § 605. Indeed, had Congress explored the question, it no doubt would have recognized, as Judge Gibbons' extensive discussion may well

indicate, that any action by it that arguably would hamper—since as we have previously concluded § 605 is intended to prohibit surveillances generally—the President's effective performance of his duties in the foreign affairs field would have raised constitutional questions. We do not intimate, at this time, any view whatsoever as to the proper resolution of the possible clash of the constitutional powers of the President and Congress. Instead, we merely note that the absence of legislative consideration of the issue does suggest that Congress may not have intended § 605 to reach the situation presented in the present case. In the absence of any indication that the legislators considered the possible effect of § 605 in the foreign affairs field, we should not lightly ascribe to Congress an intent that § 605 should reach electronic surveillance conducted by the President in furtherance of his foreign affairs responsibilities. This would seem to be far too important a subject to justify resort to unsupported assumptions.

[5] The Attorney General has certified, Ivanov does not deny, and the district court has found, that the surveillances at issue here "were conducted and maintained solely for the purpose of gathering foreign intelligence information."³⁰ Therefore, § 605 does not render them, in and of themselves, accompanied by subsequent disclosure, unlawful.

Although decisions subsequent to *United States v. Coplon*³¹ hold that § 605 does not limit the President's powers to gather foreign intelligence information,³² we are aware that *Coplon*

wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

²⁶ U.S. Const. Art. II § 2.

²⁷ *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319-322, 57 S.Ct. 216, 75 L.Ed. 255 (1936).

²⁸ 494 F.2d—38½

²⁸ See pp. 611, 612, 615 *infra*.

²⁹ See Sen.Rep.No.781, 73d Cong., 2d Sess. 1 (1934), H.R.No.1850, 73d Cong., 2d Sess. 3 (1934).

³⁰ 318 F.Supp. 66, 70-73.

³¹ 185 F.2d 629 (2d Cir. 1950).

³² *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), rev'd on other grounds, 400 U.S. 990, 91 S.Ct. 457, 27 L.Ed.2d 438 (1971); *United States v. Hoffman*, 334 F.Supp. 504 (D.D.C.1971); *United States v. Dellinger*,

may be read to undercut the position urged here as well as in the other cases subsequent to *Coplon*. We do not, however, despite our high regard for the late Judge Learned Hand, give to that case the conclusive reading suggested by Judge Gibbons. There, the court did not consider in any detail whether wiretaps for the purpose of gathering foreign intelligence information fell within the ambit of § 605. A close reading of the briefs in *Coplon* indicates that the question was not raised. Instead, the court merely assumed that the surveillance and disclosure together were illegal under § 605.³³ In the absence of any reasoning undergirding this assumption, we do not consider it is entitled to any great precedential effect and decline to adopt it here.

III. IVANOV'S FOURTH AMENDMENT RIGHTS WERE NOT INFRINGED.

Because of our conclusion that § 605 of the Communications Act neither prohibits the President from gathering foreign intelligence information nor limits

the use to which material so obtained may be put, it becomes necessary to determine whether the surveillances producing the second set of records invaded Ivanov's Fourth Amendment rights. If the surveillances did violate Ivanov's constitutional rights, then disclosure of the records and a suppression hearing may be required under the mandate of the Supreme Court.³⁴

1. *The Applicability of the Fourth Amendment to Electronic Surveillances Conducted Pursuant to the President's Foreign Affairs Powers.*

The expansive language of *United States v. Curtiss-Wright Export Corporation*³⁵ provides support for the contention that the President is authorized to act unencumbered by the Fourth Amendment requirements of prior judicial approval and probable cause when he is dealing with national security matters.³⁶ The ramifications of *Curtiss-Wright*, however, remain somewhat enigmatic in this regard. To contend that customary Fourth Amendment analysis is to be abandoned whenever the

those specifically enumerated in the Constitution, and such implied powers as are necessary and proper to carry into effect the enumerated powers is categorically true only in respect of our internal affairs.

"Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but participation in the exercise of the power is significantly limited. In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation.

"[H]e, not Congress, has the better opportunity of knowing the conditions which prevail in foreign countries, and especially is this true in time of war. He has his confidential sources of information. He has his agents in the form of diplomatic, consular and other officials. Secrecy in respect of information gathered by them may be highly necessary, and the premature disclosure of it productive of harmful results." *Id.* at 315-320, 57 S.Ct. at 219.

Crim. No. 60 CR 180 (Mem.Op.N.D.Ill. Feb. 2, 1970), *rev'd on other grounds*, 472 F.2d 340 (7th Cir. 1972); *United States v. Butenko*, 318 F.Supp. 66 (D.N.J.1970) (the present case in the district court); *United States v. Brown*, 317 F.Supp. 531 (1970), *rev'd on other grounds*, 456 F.2d 1112 (5th Cir. 1972); *United States v. Stone*, 305 F.Supp. 75 (D.D.C.1969). Compare *United States v. Smith*, 321 F.Supp. 424 (D.C.Cal.1971) (distinguishing domestic situation); *United States v. Sinclair*, 321 F.Supp. 1074 (E.D. Mich.1971) (same) *aff'd sub nom.*, *United States v. United States District Court*, 407 U.S. 297, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972).

33. *Id.* 185 F.2d at 636.

34. See pp. 598-599 *supra*.

35. 299 U.S. 304, 57 S.Ct. 216, 81 L.Ed. 255 (1936). The Court in *Curtiss-Wright* held that the Congress' delegation to the President of the authority to prohibit the sale of weapons to certain countries engaged in hostilities with each other was not unconstitutional.

36. "The broad statement that the federal government can exercise no powers except

munications Act should not be so construed and, with respect to the constitutional question, maintains that there is Presidential power to engage in warrantless surveillance to gather foreign intelligence information.

Principled adjudication of this knotty matter cannot properly be achieved by a doctrinaire preference for one interest or the other. Both executive authority in the foreign affairs area and society's interest in privacy are of significance, and are equally worthy of judicial concern.

Rarely, if ever, do the phrases of the Constitution themselves decide cases without at least some interpretative assistance from the judiciary. The Constitution speaks through the judges, but its phrases are seldom so cabined as to exclude all flexibility. Charged with the assignment to make a choice, a judge must be responsible for the choice he makes.

The importance of the President's responsibilities in the foreign affairs field requires the judicial branch to act with the utmost care when asked to place limitations on the President's powers in that area. As Commander-in-Chief, the President must guard the country from foreign aggression, sabotage, and espionage. Obligated to conduct this nation's foreign affairs, he must be aware of the posture of foreign nations toward the United States, the intelligence activities of foreign countries aimed at uncovering American secrets, and the policy positions of foreign states on a broad range of international issues.

To be sure, in the course of such wire-tapping conversations of alien officials and agents, and perhaps of American citizens, will be overheard and to that extent, their privacy infringed. But the Fourth Amendment proscribes only "unreasonable" searches and seizures.⁵⁷

57. *United States v. Slocum*, 464 F.2d 1180, 1182 (3d Cir. 1972).

58. Nearly 85 years ago, Mr. Justice Field, speaking for the Supreme Court, observed: "To preserve its independence, and give se-

And balanced against this country's self-defense needs, we cannot say that the district court erred in concluding that the electronic surveillance here did not trench upon Ivanov's Fourth Amendment rights.⁵⁸

Accordingly, the judgment of the district court denying Ivanov's request for disclosure and an evidentiary hearing will be affirmed.

SEITZ, Chief Judge (concurring and dissenting).

I concur in affirming the district court's disposition of questions respecting the first, concededly illegal, set of surveillances. My views in this matter are well stated in Part II of Judge Aldisert's opinion.

As to the second set of surveillances, the majority has found that these wire-taps and their use to procure evidence introduced against Ivanov, assuming such use was made of them, violated neither § 605 of the Communications Act nor the Fourth Amendment. Finding the wiretaps legal, the majority has held that the district court properly refused to order disclosure to Ivanov of the logs summarizing these surveillances and that the court below also properly refused to hold an evidentiary hearing on the issue of taint. Because I believe that these matters are settled by Supreme Court decisions and that the majority in effect is "overruling" Supreme Court decisions, *sub silentio*, I dissent from the majority's affirmance of district court action respecting the second set of surveillances.

I. § 605 OF THE COMMUNICATIONS ACT

As I read the majority opinion, two conclusions support its decision that § 605 of the Communications Act has not been violated here. First, in logical or-

curity against foreign aggression and encroachment, is the highest duty of every nation, and to attain these ends nearly all other considerations are to be subordinated." *Chinese Exclusion Case*, 130 U.S. 581, 602, 9 S.Ct. 623, 630, 32 L.Ed. 1088 (1889).

UNITED STATES v. BUTENKO

609

Cite as 494 F.2d 593 (1974)

der, because wiretapping is "one means of acquiring information" that may make the President's decisions regarding foreign affairs "more likely to advance our national interests," the majority presumes that Congress did not limit the President's ability to wiretap to obtain foreign intelligence information when it adopted § 605 without explicit discussion of this use of wiretaps. Second, the majority declares that "[t]here is absolutely no indication that Congress contemplated situations where interceptions were unaccompanied by divulgences" and reasons that since Congress presumably did not intend to limit the President's use of wiretaps to stay informed regarding foreign affairs, § 605 is not violated by use of wiretap-derived evidence to secure espionage convictions. These conclusions, relied on for the majority's holding that § 605 has not been breached, do not follow from their premises and contradict Supreme Court precedent as well as the terms of § 605.

Initially, I think that insufficient attention has been paid to the section itself. Section 605 of the Communications Act, 47 U.S.C. § 605 (1970), contains four distinct prohibitions. The first prohibition is directed at employees of communications facilities and is not relevant here. Cf. *Nardone v. United States*, 302 U.S. 379, 381, 58 S.Ct. 275, 82 L.Ed. 314 (1937). The prohibition contained in the third clause of § 605 concerns unauthorized reception of communications; the second and fourth prohibitions concern interception. The Act does not define reception and interception, but, attributing to the drafters a desire that each statutory statement be meaningful and not merely repetitive, I would distinguish these terms by the point in time at which the unauthorized

participant acquires access to a communication; reception would occur following transmission, while interception would occur during transmission to and preceding reception of the communication by someone other than the interceptor. The third clause of § 605, therefore, also is inapplicable here.

§ 605: Clause 2, Element (1)

If the government has violated § 605, then, it must be by virtue of the section's second or fourth prohibition. The second part of § 605 forbids (1) any person not authorized by the sender (2) to intercept and (3) divulge or publish the communication's contents, meaning or existence (4) to any person.¹ This portion of § 605 was construed by the Supreme Court in *Nardone v. United States*, *supra*, which involved in-court testimony by federal agents as to the contents of communications intercepted by government wiretaps. The argument advanced by the government in *Nardone* bears a striking resemblance to the first argument accepted by the majority here. The government contended that the executive branch was charged to take care that the laws of the United States be faithfully executed, that Congress at the time it passed the Communications Act was aware of the government's use of wiretap evidence to faithfully execute federal criminal laws, that Congress did not mention this use of wiretaps in considering § 605 of the Communications Act, and that, therefore, Congress must be presumed to have excluded federal agents, acting in furtherance of their duty to enforce criminal laws, from those persons covered by § 605. *Id.* at 381-383, 58 S.Ct. 275.

The Court in *Nardone* observed that not only was there no discussion in

1. Section 605 is written as a single sentence composed of four separable sentences joined by semi-colons and a proviso, not relevant here, modifying the entire section. For ease of discussion, I have numbered the separable sentences, each constituting a self-contained prohibition of different actions, in the order set forth in the statute and also assigned numbers to the elements required for viola-

tion of each prohibition. The second prohibition reads:

... and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person:

47 U.S.C. § 605 (1970).

adoption of § 605 of the use federal agents made of wiretaps, but there was no record of any legislative discussion concerning adoption of § 605. The Court further noted that several bills designed explicitly to prohibit government wiretapping had failed shortly before passage of the Communications Act. These circumstances, however, were insufficient to overcome "the fact that the plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that 'no person' shall divulge or publish the message or its substance to 'any person.'" *Id.* at 382, 58 S.Ct. at 276 [emphasis in original]. In explaining its refusal in the absence of legislative history to speculate that Congress intended to exclude federal agents from the strictures of § 605, the Court added:

It is urged that a construction be given the section which would exclude federal agents since it is improbable that Congress intended to hamper and impede the activities of the government in the detection and punishment of crime. The answer is that . . . Congress may have thought it less important that some offenders go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty.

Id. at 383, 58 S.Ct. at 276.

I am unable to see any difference between the argument rejected by the Supreme Court in *Nardone* and that accepted by the majority here. Both argue that the plain all-inclusive language of the statute covering any person should be construed not to apply to federal officers performing tasks assigned by the Constitution to the executive branch. Both rely on the absence of legislative history, and both would require explicit legislative consideration of a limitation on the executive's freedom of action before a statute could be read to restrict it. The canons of statutory construction considered by the Supreme Court in

Nardone, *id.* at 383, 58 S.Ct. 275, apply with equal force in both cases.

There is of course a distinction between this case and *Nardone*. The case before us, as cast by the majority, involves Presidential powers over foreign affairs, while *Nardone* concerned executive authority over domestic matters. This distinction, however, makes no legal difference. The only constitutional provision cited by the majority as authority for the executive decision-making that "foreign intelligence information" supposedly aids is Article II, section 2's declaration that "[t]he President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States" This provision certainly cannot be said to be any more important than Article II, section 3's charge that the President "take care that the Laws be faithfully executed," nor can wiretapping be deemed any more crucial to accomplishment of the President's duties as Commander-in-Chief than to his faithful execution of the laws.

The majority, however, apparently attaches significance to the fact that the President has powers over foreign affairs that are not made express in the Constitution. The majority's principal authority as to this point is *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 57 S.Ct. 216, 81 L.Ed. 255 (1936), decided one year before *Nardone*. *Curtiss-Wright* stated that the federal government possessed certain powers over foreign affairs inherent in national sovereignty. *Id.* at 318, 57 S.Ct. 216. In upholding a statute permitting the President to make certain decisions bearing on foreign affairs against a charge of unconstitutional delegation of legislative power, the Court observed that power over foreign affairs was not legislative alone. *Id.* at 319-322, 57 S.Ct. 216. While rejecting the statement in *Curtis-Wright* that certain foreign affairs powers inhere in national sovereignty, constitutional considerations

UNITED STATES v. BUTENKO

611

Cite as 494 F.2d 593 (1974)

aside, (see note 37 of the majority opinion), the majority here relies on *Curtiss-Wright* for the proposition that foreign affairs powers may be implied in the Constitution even if federal powers over domestic affairs must be express. Yet, the majority never explains why this nebulous federal implied power, even assuming that it is addressed solely to the executive, is entitled to greater deference than an express power of the executive such as *Nardone* involved.

Perhaps the majority has concluded that Congress could not limit the President's power to wiretap in order to obtain foreign intelligence information.² Without explicitly stating this conclusion, the majority indicates that "any action by [Congress] that arguably would hamper . . . the President's effective performance of his duties in the foreign affairs field would have raised constitutional questions." The majority does not cite any precedent supporting this statement, nor does it state what questions would be raised. As I read Articles I and II of the Constitution, the Congress as well as the President has powers in foreign affairs. Congress is empowered to regulate commerce with foreign nations, to define and punish crimes committed on the high seas and offenses against the law of nations, to declare war, to raise and support armies, provide and maintain a navy, to provide for calling forth the militia to repel invasions, and to make rules for governing the armed forces. The President's powers in the foreign affairs area, independent of legislative delegations, are far more limited: he is Commander-in-Chief of the armed forces and receives public ministers; he can make treaties, with the Senate's concurrence, and appoint ambassadors, again with Senate approval.

2. While the majority has added a disclaimer of this conclusion, the intimation that such a conclusion might fairly be reached is essential to the majority's position. If Congress can limit executive actions useful to foreign affairs operations, there is no basis for dis-

The President is certainly no "Lone Ranger" in the foreign affairs field, possessed, as the majority intimates, of vast constitutional powers to be exercised independently of Congress. All of the federal government's powers, including foreign affairs powers, are subject to constitutional limitations. *United States v. Curtiss-Wright Export Corp.*, *supra*, 299 U.S. at 320, 57 S.Ct. 216, and one such limitation on the President's power is the exercise of Congressional power. "When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system." *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-638, 72 S.Ct. 863, 871, 96 L.Ed. 1153 (1952) (Jackson, J., concurring) [footnote omitted].

I cannot conceive of any power in the foreign affairs field that the President exercises exclusively and for which wiretapping is essential; I cannot perceive any legal basis for intimating that Congress could not constitutionally limit the President's power to wiretap to obtain "foreign intelligence information." Apparently, Judge Learned Hand was of the same view, as were the judges concurring in his opinion in *United States v. Coplon*, 185 F.2d 629 (2d Cir. 1950). *Coplon* was, like this case, an espionage case involving the possible use of wiretap fruits. As the majority notes,

tinguishing *Nardone* from this case. *Nardone* certainly does not reflect fear of reading § 605 to mean what it says because such a reading would raise constitutional questions—yet the Court clearly allowed Congressional restriction of executive action.

Judge Hand engaged in no lengthy discussion to distinguish foreign intelligence wiretaps from others. It is safe to assume that Judge Hand knew that "foreign intelligence" was probably sought in wiretapping that led to an espionage charge. One may also assume that the government did not argue that Congressional limitation of foreign affairs wiretapping was constitutionally different from limitation of other government wiretapping—indeed, the government has not raised the argument in this case. Instead of inquiring into the constitutionality of the law, which, if he had doubted the Act's constitutionality, he would have been required to do, *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 175-180, 2 L.Ed. 60 (1803), Judge Hand declared that the validity of the *Coplon* wiretap was covered by the ruling in *Nardone*. *United States v. Coplon*, *supra*, 185 F.2d at 636.

Like Judge Hand, I can see no basis for distinguishing *Coplon* from *Nardone*, nor can I distinguish this case from those. Thus, perceiving no difference between this case and *Nardone*, I would find that the federal agents involved here fall within the category of persons described in the first element of § 605's second clause.

§ 605: Clause 2, Elements (3) & (4)

The government does not dispute that it falls within the second element of § 605's second prohibition; federal agents did intercept communications involving Ivanov. The government contends, however, that federal agents did not divulge the communication's contents to any other person, the third and fourth elements required for violation of § 605, clause two. Of course the agents who made the interception divulged the "existence, contents, substance, purport, effect, or meaning" of the intercepted communication to other agents. Perhaps, as Judge Aldisert implies, such divulgence does

3. The fourth prohibition provides:
 . . . and no person having received such intercepted communication or having

not violate § 605 because the federal officers are really acting as agents of the executive in making the interception and the relevant "person" to be viewed as interceptor is, thus, the executive; divulgence to other agents of the executive, who receive the information in such capacity, hence would not violate the statute because the "divulgees" would be part of the same "person" as the "divulgors." Cf. 47 U.S.C. § 153(i) (1970) (defining "person" to include, as well as individuals, partnerships, associations, trusts and corporations).

I do not think that question needs to be resolved here. Ivanov argues that the relevant divulgence occurred at trial when the government introduced evidence obtained by use of the wiretaps. The Supreme Court's first *Nardone* decision held that the government could not introduce testimony on the content of wiretaps. The second *Nardone* decision, *Nardone v. United States*, 308 U.S. 338, 60 S.Ct. 266, 84 L.Ed. 307 (1939), held that the fruits of the interception also could not be introduced. *Id.* at 340-341, 60 S.Ct. 266. Assuming that the Court was again dealing with the second prohibition contained in § 605, I would read *Nardone II* as holding that the use of a wiretap's fruits in court constituted a divulgence prohibited by § 605.

§ 605: Clause 4

While the precise ground for the *Nardone II* decision is not clear to me, the illegality of any derivative evidentiary use of wiretaps is. This illegality becomes more apparent on examination of the final prohibition contained in § 605. The section's last clause forbids (1) any person who has received or become aware of the existence, meaning or contents of a communication (2) intercepted without the sender's authorization (3) from divulging, publishing or using such information (4) for his own benefit or the benefit of another unauthorized person.³

become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that

UNITED STATES v. BUTENKO

613

Cite as 494 F.2d 593 (1974)

This clause expressly prohibits the use of wiretap information.

The only remarks Supreme Court justices have made referring expressly to this clause are contained in the dissent to *Goldstein v. United States*, 316 U.S. 114, 62 S.Ct. 1000, 86 L.Ed. 1312 (1942). The majority in *Goldstein* decided that defendants who were not parties to the communication lacked standing to object to introduction of wiretap fruits against them. *Id.* at 121-122, 62 S.Ct. 1000. In dissent, Justice Murphy, joined by Chief Justice Stone, who voted with the majorities in *Nardone I* and *II*, and Justice Frankfurter, who authored *Nardone II*, disagreed with the Court on standing and thus reached the merits. The dissenters found this fourth part of § 605 to be "unequivocal and controlling." 316 U.S. at 125-126, 62 S.Ct. 1000. "In enacting § 605, Congress sought to protect society at large against the evils of wiretapping and kindred unauthorized intrusions into private intercourse conducted by means of the modern media of communication, telephone, telegraph, and radio. To that end the statute prohibits not only the interception and the divulgence of private messages without the consent of the sender, but also the use of information so acquired by any person not entitled to it." *Id.* at 125, 62 S.Ct. at 1006. I would, therefore, find that § 605 prohibits use of wiretap information to obtain any evidence for trial.

§ 605: Hearing & Disclosure

Since the derivative use of wiretaps alleged by Ivanov is made illegal by § 605, the question of illegality becomes identical to the question of taint. The wiretap information must be disclosed to the defendant and a hearing must be held to resolve the issue of taint. *Alderman v. United States*, 394 U.S. 165, 180-185, 89 S.Ct. 961, 22 L.Ed.2d 176

such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect or meaning of the same or any part thereof, or use the same or any information contained therein

(1969); *Nardone v. United States*, 308 U.S. 338, 341-342, 60 S.Ct. 266, 84 L.Ed. 307 (1939); *United States v. Coplon*, *supra*, 185 F.2d at 636-640.

Since the decision in *Alderman*, the Congress has purportedly changed the method for determining taint from government wiretapping. The Organized Crime Control Act of 1970 provides, in relevant part, that taint from surveillances prior to the effective date of the Omnibus Crime Control and Safe Streets Act of 1968 shall be determined by disclosure and hearing only if an *in camera* proceeding convinces the judge that the surveillances are arguably relevant, 18 U.S.C. § 3504(a)(2) (1970), and that courts shall not consider claims that such surveillances have tainted the evidence of a crime occurring more than five years after the surveillance, 18 U.S.C. § 3504(a)(3) (1970). The bar to consideration of taint is inapplicable here since the relevant wiretaps occurred within two years of the acts sought to be proved,⁴ allegedly with wiretap fruits. The question is presented, however, whether the 1970 Act's procedure for determining taint governs this case and, if so, whether it is constitutional.

Congress specifically provided that the 1970 Act applies, to all proceedings, whenever commenced, after its effective date. Organized Crime Control Act of 1970, ch. 223, 84 Stat. 935, § 703. Congress also clearly intended to alter the procedure set forth in *Alderman* for determining taint from pre-1968 wiretaps. H.R.Rep.No.91-1549, in 1970 U.S. Code Cong. & Admin.News, pp. 4007, 4027. The precise question here, however, is whether Congress intended to change the rule of *Alderman* for the cases actually before the Court and as to evidence introduced, and to which objection was made, before passage of the 1970 Act.

for his own benefit or for the benefit of another not entitled thereto.

⁴ 18 U.S.C. § 605 (1970).

⁴ Letter of June 2, 1969 from Attorney General Mitchell.

The statute's wording would support restricting use of its procedure for determining taint to cases in which prospective admission of evidence was the subject of controversy; it applies "upon a claim by a party aggrieved that evidence is inadmissible" 18 U.S.C. § 3504(a)(1) (1970). Nothing I have found in the legislative history of the 1970 Act indicates that Congress intended the Act to apply to determinations, after its passage, on the propriety of the introduction of evidence before passage of the 1970 Act. While the statute as relevant here does not purport to change the propriety of admission of evidence, but rather changes only the method for determining admissibility, the *Alderman* Court recognized that the method of ascertaining taint may well determine whether evidence is admitted or excluded. See *Alderman v. United States*, *supra*, 394 U.S. at 183-185, 89 S.Ct. 961.

Not only do I find limitation of the 1970 Act to questions of introduction of evidence after the Act's effective date plausible, but also I find such construction necessary to avoid serious doubt as to the statute's constitutionality. I cannot dismiss *United States v. Klein*, 80 U.S. (13 Wall.) 128, 20 L.Ed. 519 (1872), as a case dealing solely with the Supreme Court's right to determine the effect of a presidential pardon. *Klein* involved three questions concerning the effect of Congressional enactments. The first question was the effect of an 1867 statute on the President's pardon powers. *Id.* at 141-142. The second question was the effect of an 1870 statute on the Supreme Court's jurisdiction. *Id.* at 143-148. The final question was the effect of the 1870 act's provisions prescribing the evidence that could be relied upon for certain findings and the result required on the basis of other findings. *Id.* The Court of Claims had, in 1869, rendered a decision in *Klein*'s favor, giving effect to the President's grant of pardon and amnesty and using evidence proscribed by the 1870 act. The Supreme Court held that the 1867

statute did not impair the President's pardon powers, and that the 1870 act neither divested the Supreme Court of jurisdiction acquired before the act's passage nor required the Court to reverse the Court of Claims decision in accordance with the statute's directive regarding the admission and effect of evidence. *Id.* I believe that *Klein* is opposite to and casts doubt upon the constitutionality of applying the 1970 Act to *Ivanov*. Because I feel that the intent of Congress that the 1970 Act apply here is not made clear by the statute's language or history and that the application of the statute to this case might not be constitutional, I would find that the 1970 Act is inapplicable to this proceeding.

II. SCOPE OF SUPREME COURT MANDATE

In suggesting disposition on § 605 grounds, I must comment on a point raised by the government for the first time in its petition for rehearing but not reached by the majority. When this case was before the Supreme Court, the Solicitor General revealed that conversations involving *Ivanov* had been overheard through wiretaps. The question of a possible § 605 violation was not raised at that time. The Supreme Court thus addressed the matter as if only a potential Fourth Amendment violation were involved. Consequently, in remanding the case to the district court, the Supreme Court directed that "[t]he District Court should confine the evidence presented by both sides to that which is material to the question of the possible violation of a petitioner's Fourth Amendment rights, to the content of conversations illegally overheard which violated those rights and to the relevance of such conversations to the petitioner's subsequent conviction." *Alderman v. United States*, *supra*, 394 U.S. at 186, 89 S.Ct. at 973. After arguing before the district court the validity of government action under § 605, the government now urges that only Fourth Amendment questions could be reached

UNITED STATES v. BUTENKO

Cite as 494 F.2d 593 (1974)

615

on remand consistent with the Supreme Court's mandate.⁵

The Supreme Court has stated that "[w]hile a mandate is controlling as to matters within its compass, on the remand a lower court is free as to other issues." *Sprague v. Ticonic National Bank*, 307 U.S. 161, 168, 59 S.Ct. 777, 781, 83 L.Ed. 1184 (1939). Such matters are open unless their "disposition . . . by the mandate . . . was necessarily implied in the claim in the original suit, and [the party's failure to raise them constituted] an implied waiver." *Id.* Since the § 605 issue was not raised prior to the remand, it was not necessarily disposed of by the Supreme Court mandate; and since the possibility of § 605 violation was not known to Ivanov at the time of his petition to the Court, his failure to raise the issue prior to remand cannot be deemed implied waiver. The obvious intent of the Supreme Court in framing its mandate was to limit proceedings on remand to issues connected with the government's wiretapping. The legality of government action under § 605 is certainly such an issue.

Finding that the case should be disposed of on § 605 grounds, I would not reach the Fourth Amendment issues.

Judge Van Dusen joins in this opinion.

Judge Aldisert joins in this opinion except the discussion contained in the section headed "§ 605: Clause 2. Element (1)."

5. It appears that the government not only argued the § 605 question before the district court without indicating that this matter might be beyond the scope of the Supreme Court's mandate, but further, the government apparently raised the matter of legality under § 605. Even if this question were arguably beyond the scope of the Supreme Court's mandate, there is some question whether the government would be estopped from arguing this question here.

1. The relevant subsections of 18 U.S.C. § 794, "Gathering or delivering defense infor-

ALDISERT, Circuit Judge (concurring and dissenting.)

I would reverse the final judgment of conviction and remand these proceedings to the district court for reconsideration. Assuming without conceding a constitutional prerogative of the Chief Executive to intercept, I am persuaded that the strictures of § 605 of the Communications Act of 1934, as interpreted by the Court in *Nardone v. United States*, 302 U.S. 379, 58 S.Ct. 275, 82 L.Ed. 314 (1937), prevents divulging or publishing the contents of the interception. My view coincides precisely with that taken by the Department of Justice under Attorneys General Tom C. Clark, J. Howard McGrath, Herbert Brownell, Jr., William P. Rogers and Robert F. Kennedy.

I.

Before proceeding into a discussion of this issue in part III, *infra*, I am constrained to set forth additional observations to present in detail the equally important issue upon which the panel of this court was not divided and upon which there appears to be unanimity in the full court: the district court's holding that the first set of logs, designated as "4001-S*" and "4002-S*" did not taint the conviction. To put these issues in proper perspective I find it necessary to set forth the facts.

Appellant Igor Ivanov, a Soviet national, was charged with having conspired with one John Butenko, an American, to violate the federal espionage statute, 18 U.S.C. § 794(a) and (c)¹

mation to aid foreign government." read as follows:

(a) Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject or citizen thereof, either directly or

(Count I), from April to October in 1963, and with having conspired to violate the statutory prohibition against acting as an agent of a foreign government without prior notification to the Secretary of State, 18 U.S.C. § 951² (Count II). Following a jury verdict of guilty, appellant Ivanov was sentenced to twenty years' imprisonment on Count I and five years' imprisonment on Count II, the sentences to run concurrently. This court affirmed the judgment of conviction against him on Count I and directed his acquittal on Count II. *United States v. Butenko*, 384 F.2d 554 (3d Cir. 1967). Appellant then filed petitions for certiorari in the United States Supreme Court. While the cases were there pending, the Solicitor General revealed that the United States had engaged in certain electronic surveillances and that Butenko and Ivanov had been overheard. The Supreme Court ordered a remand to the district court for "a hearing, findings, and conclusions (1) on the question of whether with respect to any petitioner there was electronic surveillance which violated his Fourth Amendment rights, and (2) if there was such surveillance with respect to any petitioner, on the nature and rele-

vance to his conviction of any conversations which may have been overheard through that surveillance."³ *Alderman v. United States*, 394 U.S. 165, 186-187, 89 S.Ct. 961, 973, 22 L.Ed.2d 176 (1969).

On remand, the government conceded that one set of interceptions was illegal but convinced the district court that these did not taint the conviction. The district court found a second set of interceptions to have been properly authorized by virtue of the President's prerogative to obtain foreign intelligence information, denied appellant's application for disclosure, denied an evidentiary hearing pertaining thereto, and entered a new judgment of conviction. *United States v. Ivanov*, 342 F.Supp. 928 (D.N.J.1972). This appeal followed.

The precise nature of the espionage conspiracy was a scheme to transmit to the Union of Soviet Socialist Republics the plan of a command and control system of the Strategic Air Command (SAC). Given the name "465-L," the system was being produced by International Electronic Company, a subsidiary of International Telephone and Telegraph, and was an automatic electronic system which enabled the commander of

indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by death or by imprisonment for any term of years or for life.

(c) If two or more persons conspire to violate this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

2. Whoever, other than a diplomatic or consular officer or attaché, acts in the United States as an agent of a foreign government without prior notification to the Secretary of State, shall be fined not more than \$5,000 or imprisoned not more than ten years, or both.
3. The Court also ordered:
 - The District Court should confine the evidence presented by both sides to that

which is material to the question of the possible violation of a petitioner's Fourth Amendment rights, to the content of conversations illegally overheard by surveillance which violated those rights and to the relevance of such conversations to the petitioner's subsequent conviction. The District Court will make such findings of fact on those questions as may be appropriate in light of the further evidence and of the entire existing record. If the District Court decides on the basis of such findings (1) that there was electronic surveillance with respect to one or more petitioners but not any which violated the Fourth Amendment, or (2) that although there was a surveillance in violation of one or more of the petitioner's Fourth Amendment rights, the conviction of such petitioner was not tainted by the use of evidence so obtained, it will enter new final judgments of conviction based on the existing record as supplemented by its further findings, thereby preserving to all affected parties the right to seek further appropriate appellate review.

UNITED STATES v. BUTENKO

617

Cite as 494 F.2d 583 (1974)

to alert and deploy his forces and provide him with an up to the minute picture of the total force. Additional details of the nature of this project are summarized in our earlier opinion. 384 F.2d at 557. We found that "there was substantial evidence to buttress the conviction" of Butenko, then employed as a control administrator at the International Electronic Company, and that "sufficient evidence was offered by the government to show [Ivanov's] intimate involvement with the conspiracy." 384 F.2d at 563.

At trial the government proved that on October 29, 1963, appellant was observed in Englewood, New Jersey, with two other Soviet Nationals, Pavlov and Khashin, in the vicinity of the Englewood railroad station parking lot. An automobile "driven by Butenko, drove to the railroad station lot, parked, turned off the headlights and turned on the parking lights and within a few minutes the Soviet automobile, now driven by Pavlov with Ivanov in the right front seat, came into the parking lot, signaled by turning off headlights and turning on parking lights. Here, there was a direct confrontation between Ivanov and Butenko and several minutes later, when the defendants were arrested, the briefcase of Butenko was found in the Soviet automobile." 384 F.2d at 563-564.

Two sets of logs reflecting electronic surveillances were introduced at the relevant hearing and form the backdrop of the appeal. The first set covered the

periods from May 15, 1963, to June 11, 1963, and from June 27, 1963, to August 13, 1963, and were designated as "4001-S*" and "4002-S*." These logs were disclosed to appellant. The government conceded that these logs represented illegal surveillances but contended that their use did not taint the conviction. The district court agreed. A second set of logs was not shown to appellant or his counsel but was examined by the court *in camera*. The government represented that these logs reflected intercepted conversations of Ivanov, duly obtained by the Department of Justice in the exercise of the President's right to obtain foreign intelligence information. These sealed documents, government exhibits A-1, A-2, and A-3, were accompanied by an affidavit of Attorney General John N. Mitchell setting forth the circumstances of, and authority for, the surveillance. The court ruled that this second set of logs was lawfully obtained under the theory set forth by the Attorney General and refused Ivanov the opportunity of examining them or an evidentiary hearing relating thereto.

Ivanov mounted separate arguments relating to each set of logs. He contended that the first set of logs was incomplete and, therefore, the court erred in its ruling that the use of these illegal surveillances did not taint the conviction. Secondly, he argued that the use of the surveillance evidence from the second set of logs was illegal, contravening Section 605 of the Communications Act of 1934,⁴ or, alternatively, that use

4 18 U.S.C. § 605. Unauthorized publication of communications

No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall disclose or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communication to its destination, or to proper collecting or distributing officers of the post or communicating centers over which

the communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpoena (sic) issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio, and use the same or any information therein contained for his own benefit or for the bene-

The official representatives of three Presidents—Presidents Truman, Eisenhower, and Kennedy—introduced legislation and actively beseeched Congress to amend this statute so that the government could utilize the fruits of interception in espionage cases and cases involving national security. They uniformly represented that what the Act of 1934 expressly forbade was the *divulgence* of the information received by interception, that the problem was not so much the act of interception, but the divulging in court of that which was learned from interception.

Former Attorney General Herbert Brownell, Jr., observed that after passage of the 1934 Act, "[t]he question soon arose as to whether mere interception by federal agents of messages was forbidden by Section 605. The Attorney General at that time took the view that what the law prohibited was *both* interception *and* divulgence, and that mere report of the intercepted message to public officials by FBI or other federal agents did not constitute divulgence. . . . None of the decisions [*Nardone*] rendered by the Supreme Court held that wire tapping by federal officers in and of itself was illegal, absent divulgence." Brownell, "Public Security and Wire Tapping," 39 Cornell L.Q. 195, 197, 198 (1954).¹¹

"[T]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports are not and ought not to be published to the world." *Chicago & Southern Air Lines, Inc. v. Waterman S. S. Corp.*, *supra*, 333 U.S. 103, 111, 68 S.Ct. 431, 436, 92 L.Ed. 568 (1948). The growing complexity and sophistication of modern society have led to the recognition that sophisticated techniques are required for gathering intelligence information where national security is involved. As early as 1876, the Supreme Court recognized the presidential power

to conduct intelligence operations in order to protect the security of the nation. *Totten v. United States*, 92 U.S. 105, 23 L.Ed. 605 (1876). In 1940, President Roosevelt, in a confidential memorandum to Attorney General Robert H. Jackson recognized the necessity of wiretapping in matters "involving the defense of the Nation." President Truman expressly approved this practice as have all Attorneys General since 1940.

When Secretary of State William P. Rogers was Deputy Attorney General he wrote a perceptive article which completely supports my analysis that there is a basic distinction under § 605 between the right to intercept and the right to use interceptions as evidence. Rogers, "The Case for Wire Tapping" 63 Yale L.J. 792 (1954): "It has long been the position of the Department of Justice that mere interception of telephone communications is not prohibited by federal law." 63 Yale L.J. at 793. Mr. Rogers outlined the long struggle of Attorneys General to persuade Congress to enact legislation to permit the introduction into evidence of intercepted communications in criminal prosecutions. "Attorney General J. Howard McGrath submitted wire tap legislation for introduction in the 82d Congress. In doing so, he repeated [a plea of former] Attorney General Clark and indicated that such legislation would 'enable the prosecution of present, future, and past violations of laws endangering our internal security, not barred by the statute of limitations, which would otherwise go unpunished to the detriment of the Nation.'" 63 Yale L.J. at 795.

Mr. Rogers states that Attorney General McGrath reaffirmed the inability of his department to fulfill "its statutory duty of prosecuting" and that Attorney General Herbert Brownell complained to Congress that without wiretap legislation "the hands of prosecuting officers are tied and their efforts to maintain the security of the Nation are thwart-

11. The debate on the Communications Act of 1934 did not discuss § 605. Mr. Brownell reports: "Not one word is said about making evidence obtained by wire tapping inad-

missible in evidence or about prohibiting wire tapping." See 73 Cong.Rec. 4138, 8822-8837, 8842-8854, 10304-10332 (1934). 39 Cornell L.Q. at 197 n. 10.

UNITED STATES v. BUTENKO

625

Cite as 194 F.2d 593 (1974)

ed."¹² "Again, on November 17, 1953, Attorney General Brownell advised a congressional committee that the work of the Department of Justice has clearly shown the need for legislation which would permit the use of wire tap evidence in espionage cases. He advised that there are cases of espionage presently in the Department of Justice but that since some of the important evidence was obtained by wire tapping, such cases could not be brought to trial so long as the law remains in the present state." 63 Yale L.J. at 796. (Emphasis supplied.) Significantly, the "law" explicitly referred to by Mr. Rogers and Attorney General Brownell was the instruction contained in the *Nardone* cases, as amplified by *Weiss v. United States*, 308 U.S. 321, 60 S.Ct. 269, 84 L. Ed. 298 (1939), applying the doctrine to intrastate as well as interstate communications. 62 Yale L.J. 793 nn. 5, 6, and 7.

The efforts of the various Attorneys General came to fruition with the passage of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, *supra*. Unlike § 605, the present wiretap statute, 18 U.S.C. § 2511(3), note 6, *supra*, contains a provision providing for the evidentiary use of intercepted communications: "The contents of any wire or oral communication intercepted by authority of the President in the exercise of . . . [his constitutional] powers may be received in evidence in any trial hearing. . . ." ¹³

Attorney General Robert F. Kennedy testifying before Congress on May 22, 1962, in support of H.R. 10185, dramatically pin-pointed the deficiencies in § 605:

12. Letter of May 7, 1953, to the Speaker of the House of Representatives and the Vice President, transmitting a wiretap legislative proposal.

13. I emphasize again that I do not meet the constitutional issue of the President's power under Title III of the Act of 1968 to wiretap without a court order to gather foreign intelligence information, the question reserved in *United States v. United States District Court*, *supra*.

494 F.2d—40

Why do I say the existing situation is unsatisfactory?

The existing federal law on wiretapping is Section 605 of the Communications Act of 1934, which provides in part:

" . . . no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person . . ."

This law is unsatisfactory in two respects. It permits anyone to tap wires. Mere interception is not a crime; a crime is not committed until the intercepted information is divulged or published. (Another provision makes it a crime to use such information for one's own benefit.)

Thus even if we find an intercepting device attached to a telephone line, and find out who is doing the intercepting, we still cannot prosecute. We have to find that the information was divulged or published or used improperly. This means that no one's privacy is adequately protected. Anyone can listen in to your telephone conversations, and mine, without violating the federal law.

On the other hand, all divulgence is prohibited. *This means that it is against the law for law enforcement officials to disclose in court any of the words they overhear from wiretapping or the substance, purport, or effect of those words—even though what they overhear is clear evidence of a vicious crime.*

Section 605 does not appear to inhibit the Chief Executive from fully conducting the necessary operations within the framework of the Executive Branch, other than the use of the evidence in prosecutions. Thus, in the case at bar, Gleb Pavlov, Yuri Romashin, and Vladimir Olenov, who were named as co-conspirators but not defendants in the indictments, were accredited representatives of the Permanent Mission of the Union of Soviet Socialist Republics to the United Nations. They were declared *persona non grata* and departed the United States.

The Supreme Court so held with respect to federal officers in the *Nardone* case, decided in 1937. And it so held with respect to state officers in the *Benanti* case, decided in 1957. Indeed, the federal courts refuse to receive in evidence, not only the substance of the intercepted conversation, but any evidence obtained as a result of leads which that conversation gave. As a result, wiretapping cannot be used effectively by the federal government or the states to aid in law enforcement, even for the most serious crimes.

The strange paradox is that under this federal law a private individual is free to listen in to telephone conversations for the most improper motives, but law enforcement officials cannot use wiretapping effectively to protect society from major crimes.

Hearings on Nominations of William H. Rehnquist and Lewis F. Powell Before the Senate Committee on the Judiciary, 92nd Cong., 1st Sess., at 145 (1971). (Emphasis supplied.)

Attorney General Kennedy stated that the passage of the bill was needed for national security cases:

Wiretapping is an important tool in protecting the national security. In 1940, President Roosevelt authorized Attorney General Jackson to approve wiretapping in *national security cases*. Attorney General Clark, with President Truman's concurrence, extended this authorization to kidnapping cases.

As Congress has been advised each year by the Director of the Federal Bureau of Investigation, the practice has continued in a limited number of cases upon express permission from the Attorney General. But, as I have pointed out, the evidence received from these wiretaps or developed from leads resulting from these wiretaps cannot be used in court. It is an anomalous situation to receive information of a heinous crime and yet not be able to use that information in court.

And, of course, this applies not only in cases of *espionage and treason* but

in pressing the fight against organized crime.

H.R. 10185 would authorize wiretapping and introduction of wiretap evidence in court for the following federal offenses:

Crimes affecting the national security: *Espionage, sabotage, treason, sedition, subversive activities and unauthorized disclosure of atomic energy information;*

Ibid., at 146-147. (Emphasis supplied.)

I am persuaded, therefore, that the district court erred in equating an assumed presidential power to intercept with the right to "divulge or publish" that which was intercepted. I would hold that assuming a constitutional prerogative of the Chief Executive to intercept, the doctrine of *Nardone* prevents, under strictures of § 605, divulging or publishing the contents of the interception. In this context any use of the intercepted material beyond the confines of the Executive Branch would have been contrary to the statutory prohibition. I would remand these proceedings to the district court for reconsideration in accordance with the foregoing analysis.

On the present state of the record I would agree with the government's contention that additional overhearings of Ivanov's conversations following his conviction were not within the mandate for disclosure of "electronic surveillance which might have violated defendants' Fourth Amendment rights and tainted their convictions."

Judge Van Dusen joins in this opinion.

GIBBONS, Circuit Judge (dissenting in part).

I concur in the court's determination that the district court did not err in concluding that the evidence used at Ivanov's trial was not the tainted fruit of anything heard in the electronic surveillances the contents of which are preserved in the first set of logs. I dissent from the majority's conclusion that the

The Supreme Court so held with respect to federal officers in the *Nardone* case, decided in 1937. And it so held with respect to state officers in the *Benanti* case, decided in 1957. Indeed, the federal courts refuse to receive in evidence, not only the substance of the intercepted conversation, but any evidence obtained as a result of leads which that conversation gave. As a result, wiretapping cannot be used effectively by the federal government or the states to aid in law enforcement, even for the most serious crimes.

The strange paradox is that under this federal law a private individual is free to listen in to telephone conversations for the most improper motives, but law enforcement officials cannot use wiretapping effectively to protect society from major crimes.

Hearings on Nominations of William H. Rehnquist and Lewis F. Powell Before the Senate Committee on the Judiciary, 92nd Cong., 1st Sess., at 145 (1971). (Emphasis supplied.)

Attorney General Kennedy stated that the passage of the bill was needed for national security cases:

Wiretapping is an important tool in protecting the national security. In 1940, President Roosevelt authorized Attorney General Jackson to approve wiretapping in *national security cases*. Attorney General Clark, with President Truman's concurrence, extended this authorization to kidnapping cases.

As Congress has been advised each year by the Director of the Federal Bureau of Investigation, the practice has continued in a limited number of cases upon express permission from the Attorney General. But, as I have pointed out, the evidence received from these wiretaps or developed from leads resulting from these wiretaps cannot be used in court. It is an anomalous situation to receive information of a heinous crime and yet not be able to use that information in court.

And, of course, this applies not only in cases of *espionage and treason* but

in pressing the fight against organized crime.

H.R. 10185 would authorize wiretapping and introduction of wiretap evidence in court for the following federal offenses:

Crimes affecting the national security: *Espionage, sabotage, treason, sedition*; subversive activities and unauthorized disclosure of atomic energy information;

Ibid., at 146-147. (Emphasis supplied.)

I am persuaded, therefore, that the district court erred in equating an assumed presidential power to intercept with the right to "divulge or publish" that which was intercepted. I would hold that assuming a constitutional prerogative of the Chief Executive to intercept, the doctrine of *Nardone* prevents, under strictures of § 605, divulging or publishing the contents of the interception. In this context any use of the intercepted material beyond the confines of the Executive Branch would have been contrary to the statutory prohibition. I would remand these proceedings to the district court for reconsideration in accordance with the foregoing analysis.

On the present state of the record I would agree with the government's contention that additional overhearings of Ivanov's conversations following his conviction were not within the mandate for disclosure of "electronic surveillance which might have violated defendant's Fourth Amendment rights and tainted their convictions."

Judge Van Dusen joins in this opinion.

GIBBONS, Circuit Judge (dissenting in part).

I concur in the court's determination that the district court did not err in concluding that the evidence used at Ivanov's trial was not the tainted fruit of anything heard in the electronic surveillances the contents of which are preserved in the first set of logs. I dissent from the majority's conclusion that the

UNITED STATES v. BUTENKO

Cite as 494 F.2d 583 (1974)

627

tainted fruits of the electronic surveillances the contents of which are preserved in the second set of logs were admissible at his trial because the interceptions were lawful. While I agree with much that Judge Aldisert says in part III of his opinion with respect to 47 U.S.C. § 605, I find it difficult to accept the construction which separates the prohibition against interception from the prohibition against disclosure and which treats the latter as a mere rule of evidence. I agree with Judge Adams that if the statute applies to the executive functioning in the field of foreign affairs intelligence by its plain language, it prohibits both interception and disclosure. His analysis suggests that if it prohibits the executive from intercepting foreign affairs intelligence, it may be beyond the power of Congress. Thus he adopts a construction making § 605 inapplicable to the executive when functioning in the field of foreign affairs intelligence. That construction is as strained as Judge Aldisert's construction.

We . . . face the fact that the plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that "no person" shall divulge or publish the message or its substance to "any person." *Nardone v. United States*, 302 U.S. 379, 382, 58 S.Ct. 275, 276, 82 L. Ed. 314 (1937).

Judge Learned Hand had no difficulty in understanding the plain language of § 605 when in *United States v. Coplon*, 185 F.2d 629 (2d Cir. 1950), cert. denied, 342 U.S. 920, 72 S.Ct. 362, 96 L. Ed. 688 (1952), he applied it to interceptions for foreign affairs intelligence. Nor do I. As I read it, the statute by its plain language applied at the time of the interceptions here in issue to everyone including the President's agents gathering foreign affairs intelligence.

1. *Nardone v. United States*, *supra*, expressly rejected any general governmental prerogative exemption to § 605. 302 U.S. at 383, 58 S.Ct. 275. Compare with 1 W. Blackstone, *Commentaries on the Laws of Eng-*

Obviously Congress thought as much when it amended § 605 by the enactment of § 2511(3) of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2511(3). This reading requires that I confront the constitutional limitation on congressional power postulated by Judge Adams as a reason for his interpretation. He writes:

We do not intimate, at this time, any view whatsoever as to the proper resolution of the possible clash of the constitutional powers of the President and Congress. Instead, we merely note that the absence of legislative consideration of the issue does suggest that Congress may not have intended § 605 to reach the situation presented in the present case. In the absence of any indication that the legislators considered the possible effect of § 605 in the foreign affairs field, we should not lightly ascribe to Congress an intent that § 605 should reach electronic surveillance conducted by the President in furtherance of his foreign affairs responsibilities. This would seem to be far too important a subject to justify resort to unsupported assumptions. Majority Opinion at 601.

He suggests, in other words, that had it thought of the problem Congress would have recognized that there is an executive prerogative in the field of foreign affairs intelligence which is constitutionally beyond its power.¹ Thus, he reasons, we may write into § 605 an exception which is not there. I have no doubt that it was well within the power of Congress to forbid, as it did, the agents of the executive from intercepting electronic communications for any purpose, including foreign affairs intelligence. The only limitation on that power that occurs to me is the veto power of the President.

Judge Adams' interpretation of § 605 as exempting the executive's foreign af-

land 261 (5th ed. 1773), which explains that "the king is not bound by any act of parliament, unless he be named therein by special and particular words."

422 N.E.2d 506

52 N.Y.2d 638

The PEOPLE of the State of New York, Respondent,

v.

Marvin TEICHER, Appellant.

Court of Appeals of New York.

May 12, 1981.

Dentist charged with sexual abuse of patients filed motion to controvert warrant to secretly place a camera in his dental office to videotape events of patient's visits, and to suppress film of tape used at trial. The Supreme Court, Robert M. Haft, J., 90 Misc.2d 638, 395 N.Y.S.2d 587, denied motion. Defendant was thereafter convicted in the Supreme Court, New York County, Cropper, J., on two counts of sexual abuse in the first degree, and he appealed. The Supreme Court, Appellate Division, Kupferman, J., 73 A.D.2d 136, 425 N.Y.S.2d 315, affirmed, and appeal was taken. The Court of Appeals, Gabrielli, J., held that: (1) evidence was sufficient to support finding that first victim lacked capacity to consent to original touching because of her generally weakened condition and to establish element of sexual gratification under statute providing that person is guilty of sexual abuse in the first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless; (2) warrant permitting surveillance is authorized by provisions of article providing that personal property is subject to seizure pursuant to search warrant if there is reasonable cause to believe that it constitutes evidence or tends to demonstrate that an offense was committed or that a particular person participated in the commission of an offense; and (3) where probable cause was clearly established by affidavit offered by district attorney in support of his application for warrant, warrant particularly described place to be searched and things to be seized, warrant explicitly provided that surveillance be conducted in such way as to mini-

mize required activities not related to specified crimes, and there were no less intrusive means for obtaining needed evidence, warrant authorizing video electronic surveillance of dentist's office was valid.

Affirmed.

1. Assault and Battery § 92(5)

Evidence established that first victim was incapable of consenting to touching and that touching was for sexual gratification to support defendant's conviction under statute providing that a person is guilty of sexual abuse in the first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless. Penal Law § 130.65, subd. 2.

2. Assault and Battery § 59

Defendant's act of placing victim's hand against his genital area constituted crime of sexual abuse under statute providing that a person is guilty of sexual abuse of first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless. Penal Law § 130.65, subd. 2.

3. Assault and Battery § 92(5)

Evidence was sufficient to prove that second victim was incapable of consenting by reason of being physically helpless under statute providing that a person is guilty of sexual abuse of first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless. Penal Law § 130.65, subd. 2.

4. Assault and Battery § 65

Second victim's status as a police decoy did not result in implicit consent to physical touching on ground that she voluntarily placed herself in a position to incur such abuse for purposes of statute providing that a person is guilty of sexual abuse of first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless. Penal Law § 130.65, subd. 2.

83 N.Y.2d 643

PEOPLE v. TEICHER

847

Cite as, Ct.App., 439 N.Y.S.2d 846

5. Assault and Battery ⇐92(5)

Where visual material on tape did not disprove conclusion that an unlawful touching occurred, even though camera angle precluded an unobstructed view of all of defendant's activities, and trier of fact was entitled to consider police inspector's testimony as direct evidence that described touching actually occurred, there was sufficient proof that an improper touching occurred for purposes of statute providing that a person is guilty of sexual abuse in first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless. Penal Law § 130.65, subd. 2.

6. Assault and Battery ⇐63

Trier of fact had more than ample basis for rejecting contention of defendant, who was convicted under statute providing that a person is guilty of sexual abuse in the first degree when he subjects another person to sexual contact when the other person is incapable of consent by reason of being physically helpless, that touching of second victim was performed pursuant to a valid medical procedure. Penal Law § 130.65, subd. 2.

7. Telecommunications ⇐519

Warrant authorizing video electronic surveillance was valid under provisions of article stating that personal property is subject to seizure pursuant to a search warrant if there is reasonable cause to believe that it constitutes evidence or tends to demonstrate that an offense was committed or that a particular person participated in the commission of an offense. CPL 690.10, subd. 4.

8. Telecommunications ⇐491

Even though federal wiretapping statute preempts state law in area of electronic surveillance, statute did not prohibit video electronic surveillance of defendant's office, in that statute does not apply to field of video electronic surveillance. 18 U.S.C.A. §§ 2510-2520.

9. Telecommunications ⇐491

Even though there is a high degree of intrusiveness inherent in video electronic surveillance, such activities are not per se unreasonable and need not be prohibited under all circumstances. U.S.C.A. Const. Amend. 4.

10. Telecommunications ⇐515

Where there was probable cause to believe that defendant was committing, had committed, or was about to commit crime of sexual abuse in the first degree, crime under investigation was specified type of activity sought to be captured by camera and person expected to be seen performing activity was specified, surveillance was confined to observation of activities for which the warrant was issued, and there were no less intrusive means for obtaining the needed evidence, warrant authorizing video electronic surveillance of dentist's office was valid.

└Jacob W. Heller and Eli Feit, New York City, for appellant. 1409

└Robert M. Morgenthau, Dist. Atty. (Robert M. Pitler and David H. Steiner, New York City, of counsel), for respondent. 1411

└OPINION OF THE COURT 1413

GABRIELLI, Judge.

The present appeal arises out of nonjury trial of a dentist who stands convicted of sexually abusing two female patients while they were under the effects of sedation at defendant's office. A camera, which had been secreted in defendant's treatment room pursuant to a warrant, recorded one of the alleged incidents of sexual abuse. Several issues are raised on appeal, including the propriety of admitting into evidence a video tape of defendant's activities. In affirming defendant's conviction, we hold today that a warrant may issue to authorize the video taping of evidence to be admitted at a subsequent trial, provided certain procedures are followed and certain safeguards are observed.

The defendant, a dentist practicing in Manhattan, was convicted of two counts of sexual abuse in the first degree (Penal Law, § 130.65, subd. 2) for allegedly subjecting two female patients to sexual contact while they were "incapable of consent by reason of being physically helpless". ¹⁶⁴³ The indictment upon which defendant was tried contained three counts of sexual abuse predicated upon the complaints of three of defendant's patients: Susan Hyman, Randi Carson and Dorothy Beineix. Each of the complainants alleged that they were subjected to physical contact of a sexual nature as they were recovering from the effects of sedation administered by defendant.

Susan Hyman first went to defendant's office to have a wisdom tooth extracted. After she expressed her fear that novocaine would not sufficiently deaden her pain, Dr. Teicher offered to use another method. Then, presumably to determine if she would suffer any adverse effects from the administration of a general sedative, he performed several tests on his patient and thereafter injected a fluid into her arm causing her to lose consciousness.

At trial Hyman testified that she awoke from her state of unconsciousness when she heard someone calling her name and felt something was touching her face. She opened her eyes and saw an exposed penis directly in front of her. Closing her eyes again, she reopened them to see a pair of trousers being zipped shut. Defendant then slapped her face, touched her blouse and lifted her from the dental chair. Hyman was still groggy and could not control her arms and legs. Defendant told her to "ventilate" her arms and he then drew her close to him and kissed her. While the patient was still unable to stand, defendant, while supporting her body, moved his hands over her breasts and thighs.

Several days following this encounter Ms. Hyman reported the incident to the police. The police equipped her with a hidden microphone before her next visit to the dentist, but when she questioned defendant about his prior activities he refused to admit that he had sexually assaulted her. He

did, however, ask Ms. Hyman to join him at his hotel room. She refused his invitation, agreeing instead to meet with him at a nearby bar. On this next rendezvous Hyman was once more equipped with a recording device, but once again defendant made no admission of illegal conduct.

The police also received a complaint from Randi Carson, who had initially gone to defendant's office for an examination and X rays and later returned for further treatment. ¹⁶⁴⁴ As in Ms. Hyman's case, the defendant gave Ms. Carson a drug, which caused her to lose consciousness immediately. When she awakened she was assisted into a recovery room and, while she was resting there and still overcoming the effect of the drug which had been injected, defendant entered the room and closed the door behind him. No one else was present. Defendant at first tried to lift Carson to a standing position, but his efforts were unsuccessful. He then lifted her hand and placed it on his pants directly over his penis. Although she was still weak, Carson testified she was able to pull her hand away. Carson also testified that defendant kissed her during this encounter and made a remark which she understood as a request to perform an act of oral sex. In addition, according to Carson, he repeatedly asked her to meet with him at his hotel room. Later, upon arriving home, Carson noticed that her underwear was wet and that there was a soreness on the left side of her vagina which she had not felt before her visit to the doctor. That evening Carson brought her complaints to the police.

Carson later returned to defendant's office wearing a hidden microphone supplied by the police, but no further acts of sexual abuse were recorded or observed by the patient. After this visit defendant telephoned Carson several times at her home to ask her if he could visit with her. Finally, Ms. Carson again returned to defendant's office with a microphone. In response to her attempts to elicit admissions of sexual abuse from the dentist, however, defendant told her only that the drug he had injected had caused her to imagine the incident of which she later testified.

As a result of these complaints by Hyman and Carson and the unsuccessful efforts of the police to obtain additional incriminating evidence against the dentist, the District Attorney's office obtained a warrant authorizing the police to install a camera in defendant's office to monitor his treatment of patients who had consented to the taping. Pursuant to a prearranged plan, Police Officer Dorothy Beineix then went to defendant's office and made an appointment to ¹⁸⁴⁵ have a wisdom tooth extracted at a later date. On the morning of Officer Beineix' appointment, the police entered defendant's office and installed the camera in a ceiling ventilator in one of defendant's examining rooms. The camera, which was focused on the dentist's chair, was connected to a video recorder and was monitored by police officers who were waiting in the basement of the building.

Later that morning, Ms. Beineix returned to defendant's office to keep her appointment. Defendant first checked her pulse and blood pressure and then lifted her blouse to examine her chest with his stethoscope. During this preliminary examination he instructed her that if she began to have difficulty breathing she should stand, lift her arms and breathe deeply. Following the examination, defendant administered a drug which caused Beineix to lose consciousness. While Beineix was unconscious defendant extracted her tooth and, at one point during this procedure, lifted her blouse and again examined her bare chest with his stethoscope. During this entire period, defendant and Ms. Beineix were alone in the treatment room. As Ms. Beineix began to regain consciousness, defendant asked her to stand and put her arms around him. Since she had no control over her body at this time, Beineix told the doctor that she was unable to stand. Defendant then lifted her out of the dental chair and pulled her towards him. While sitting on a stool in front of the dental chair with Ms. Beineix between his legs, defendant lifted her blouse and began moving his hands across the upper part of her back and around toward her breasts. He then slid both hands down across her back and

grabbed her buttocks. While massaging her buttocks in a circular motion he drew her body toward his. All of these actions were recorded on the video tape which was later admitted into evidence.

At this point the officers who were monitoring the video tape in the basement signaled other officers to arrest defendant. Detective Brech and Investigator Dadona were the first to enter the treatment room. Dadona testified at trial that when he first opened the door he observed that defendant's hands were on Ms. Beineix' sides, and that his thumbs were massaging the nipples of her breasts.

¹⁸⁴⁶ At his subsequent trial defendant was convicted of two counts of sexual abuse in the first degree for the acts committed upon complainants Carson and Beineix. The count involving the complaint of Susan Hyman was dismissed, however, because the court found that defendant's guilt had not been established beyond a reasonable doubt. A divided Appellate Division affirmed defendant's conviction on both counts, and leave to appeal to this court was thereafter granted. Defendant now attacks the judgment of conviction on several grounds.

[1] Defendant first contests his conviction on the count concerning the Carson incident on the ground that the evidence at trial was insufficient, as a matter of law, to establish his guilt. The statute under which defendant was convicted provides that a person is guilty of sexual abuse in the first degree when he subjects another person to sexual contact "[w]hen the other person is incapable of consent by reason of being physically helpless" (Penal Law, § 130.65, subd. 2). Sexual contact is defined in the Penal Law as "any touching of the sexual or other intimate parts of a person not married to the actor for the purpose of gratifying the sexual desire of either party" (Penal Law, § 130.00, subd. 3). Defendant claims that the evidence at trial was insufficient to establish that Ms. Carson was incapable of consenting to the touching and that there was no evidence to establish that

this touching was for sexual gratification. Neither of these claims is supported by the record.

Carson was heavily sedated at the time the initial touching occurred and, as a consequence, she was in an extremely weakened condition. Thus, although she had enough control over her body to pull her hand away after defendant had placed it against his penis, the trier of fact was entitled to infer that she lacked capacity to consent to the original touching because of her generally weakened condition. Furthermore, we find defendant's contention that the touching was too fleeting to establish the element of sexual gratification to be frivolous. The statute does not require that actual gratification occur, but only that the touching be for that purpose. Defendant's act of placing his patient's hand ¹⁶⁴⁷ against his covered penis was more than sufficient to permit a trier of fact to find that the purpose of this act was sexual gratification.

[2] Defendant also argues that even if the element of sexual gratification and the victim's incapacity were established, his act of placing Carson's hand against his genital area could not possibly constitute the crime of sexual abuse, since the statute proscribes only the act of a defendant who touches the intimate parts of his victim and not the act of a person who places his victim's hand against his own intimate parts. As we have held, this argument must be rejected because it requires an overly restrictive and improper reading of the statutory language (see *People v. Ditta*, 52 N.Y.2d 657, 439 N.Y.S.2d 855, 422 N.E.2d 515). The common-law policy that a penal provision should be strictly construed has been expressly abolished by the Legislature; instead penal statutes are to be interpreted "according to the fair import of their terms to promote justice and effect the objects of the law" (Penal Law, § 5.00) and are not to be given hypertechnical or strained interpretations (*People v. Ditta*, *supra*, citing *People v. Sansanese*, 17 N.Y.2d 302, 306, 270 N.Y.S.2d 607, 217 N.E.2d 660; *People v. Wood*, 8 N.Y.2d 48, 51, 201 N.Y.S.2d 328, 167 N.E.2d 736).

Addressing the other count upon which defendant was convicted, that involving the sexual abuse of Dorothy Beineix, defendant once more challenges the sufficiency of the evidence, and also asserts that, for various reasons, the introduction into evidence of a video tape of his actions relating to the Beineix incident was improper. For reasons which follow we also uphold defendant's conviction under this count of the indictment.

The evidence upon which the People's case was built consisted primarily of the video tape of defendant's actions, the testimony of Inspector Dadona and Dorothy Beineix and, finally, the testimony of an expert witness who attempted to refute defendant's claim that his actions were medically necessary. The camera which recorded defendant's activities was positioned in such a way as to give a view overlooking the dental chair and a portion of the room. The relevant portion of the video tape revealed that after defendant had completed the extraction of Beineix' tooth, ¹⁶⁴⁸ he lifted his patient from the dental chair and placed her between his legs. At this moment defendant was sitting atop a stool and supporting Beineix in a standing position. It could readily be inferred from a viewing of the tape that the patient had no control over her body at this point. Defendant then lifted Beineix' blouse and moved his hands across her back. Although, because of the camera angle, it cannot be determined from the tape whether defendant actually placed his hands upon Ms. Beineix' breasts, the tape does reveal that he massaged her buttocks with both hands and pulled her toward his pelvic region. In addition to the video tape, the People also produced Inspector Dadona, who entered the treatment room at the signal of the officers monitoring the video tape and was therefore able to give eyewitness testimony of what transpired. He testified that when he first entered the office he observed defendant holding Beineix by her sides and massaging the nipples of her breasts with his thumbs. Although Beineix testified at

trial that she could not recall if defendant had massaged her breasts, she was able to recall that he moved his hands across her body and down to her buttocks, causing her to become very frightened.

[3, 4] Defendant first contends that there was no proof that Beineix was incapable of consent by reason of being physically helpless. Noting that when he first told her to stand she responded that she was unable to do so, defendant argues that the crime of sexual abuse was not made out because there was no proof that Beineix could not communicate her unwillingness to submit to the subsequent touching. She did, however, testify that she had no control over her body, although she was mentally aware. As the People assert, simply because Beineix was unable to respond to defendant's direct command to stand does not prove, as a matter of law, that she was able to protest every subtle movement of his hand across her flaccid body. The People's medical expert testified at trial that when a patient is raised to a standing position, as in this case, there may be a decrease in the cerebral blood flow which could result in dizziness or even unconsciousness. In addition, the doctor testified that this effect is merely compounded by the application of chest compression. The state of the victim's physical helplessness at any given moment is largely a question of fact which, in view of this and other testimony, we may not question upon this record. Furthermore, we reject the notion that the victim's status as a police decoy resulted in implicit consent to the physical touching because, as defendant claims, she voluntarily placed herself in a position to incur this abuse. Her consent to acting as a police decoy is not equivalent to a consent to a touching of her intimate parts, which she was physically incapable of giving at the time of the illegal activity.

[5] Defendant also asserts that there was insufficient proof that any improper touching occurred because the tape was inconclusive on this point and, further, because the testimony of Inspector Dadona was not worthy of belief. The visual mate-

rial on the tape, however, did not serve to disprove, on the contrary was consistent with, the conclusion that an unlawful touching occurred, even though the camera angle precluded an unobstructed view of all of defendant's activities. And, inasmuch as Inspector Dadona's testimony was not, as a matter of law, incredible, the trier of fact was entitled to consider his testimony as direct evidence that the described touching actually occurred.

[6] Finally, defendant attacks the sufficiency of this evidence by asserting that the People have failed to prove, beyond a reasonable doubt, that the touching of Beineix was not performed pursuant to a valid medical procedure. Indeed, throughout the course of this litigation defendant's position has been that the actions which he took were part of a necessary medical treatment to bring Beineix out of a state of respiratory distress through the application of pressure on her ribcage. In support of these assertions defendant produced two experts at trial who indicated that the actions depicted on the tape could be a form of resuscitatory technique. Interestingly, they also indicated, however, that this technique was neither taught nor recommended, that it was unknown to them and, in fact, would probably be employed only by a minimally trained practitioner. Moreover, the People produced an expert witness who testified in substance that the tape reveals that Beineix was not in need of respiratory assistance and that, even if she were, the method of resuscitation employed by defendant would in fact be detrimental to his patient rather than helpful. In light of this evidence the trier of fact had more than ample basis for rejecting defendant's contention that his actions were dictated by any claimed medical necessity.

Defendant's next assertions go not to the sufficiency of the evidence at trial, but to the propriety of permitting the video tape of his activities involving Ms. Beineix to be introduced into evidence. This matter presents questions of first impression before this court.

Defendant's initial contention is that Supreme Court had no power to issue a warrant authorizing the type of surveillance which took place in this case. There is, of course, no doubt that the Supreme Court had the power to authorize the aural recording of the events in defendant's office. The authority of a court to permit aural electronic surveillance is derived from CPL article 700. This article deals with the use of eavesdropping warrants, and defines eavesdropping as wiretapping or mechanical overhearing of a conversation (CPL 700.05, subd. 1). Defendant, however, argues that article 700, by its express terms, may not be read as conferring on the courts the power to authorize video electronic surveillance.

Initially, we note our agreement with defendant's contention that CPL article 700 does not apply to video surveillance.¹ This article applies only to eavesdropping, which is defined as wiretapping or mechanical ¹⁵⁸¹overhearing of a conversation (CPL 700.05, subd. 1). The statutory language is directed toward the aural acquisition of information, and does not mention the acquisition of visual images.

[7] Nevertheless, we believe that the warrant which permitted video surveillance in this case was valid, since it was authorized by the provisions of CPL article 690. CPL 690.10 (subd. 4) provides that "[p]ersonal property is subject to seizure pursuant to a search warrant if there is reasonable cause to believe that it . . . [c]onstitutes evidence or tends to demonstrate that an

1. The police obtained the aural portions of the video tape by planting a microphone in Beineix' purse, which she carried into the treatment room. In general, if one of the parties to an intercepted conversation consents to the recording or mechanical overhearing of that conversation, the provisions of CPL article 700 do not apply (see CPL 700.05, subd. 1; Penal Law, § 250.00; see, also, *United States v. White*, 401 U.S. 747, 91 S.Ct. 1122, 28 L.Ed.2d 453). Although the fact that Beineix was unconscious during her dental treatment might have some bearing on an analysis under *United States v. White*, we have no need to consider the question since defendant does not separately contest the aural portion of the tape, perhaps because it contains little of an inculpatory nature.

offense was committed or that a particular person participated in the commission of an offense". Defendant maintains that this statute authorizes only the seizure of tangible property and does not permit the seizure of an intangible visual image secured by a video recording. We reject this interpretation.

In *People v. Abruzzi*, 52 A.D.2d 499, 385 N.Y.S.2d 94, aff'd on opn below 42 N.Y.2d 813, 396 N.Y.S.2d 649, 364 N.E.2d 1342, cert. den. 434 U.S. 921, 98 S.Ct. 396, 54 L.Ed.2d 278, the court reversed the conviction of a doctor who had been convicted for certain acts of sexual misconduct largely upon the testimony of a police officer who had observed defendant's actions while perched on a ladder outside the doctor's window. The *Abruzzi* court held that the defendant's motion to suppress this evidence should have been granted because it was procured without the authorization of a warrant. Implicit in this holding is the premise that a proper warrant may issue to permit the seizure that results from obtaining visual observations of a crime in progress in a private place. Similarly, in *United States v. New York Tel. Co.*, 434 U.S. 159, 98 S.Ct. 364, 54 L.Ed.2d 376, the Supreme Court had occasion to determine if rule 41 of the Federal Rules of Criminal Procedure, which closely parallels the language of CPL 690.10 (subd. 4), authorizes the issuance of a warrant to seize intangible evidence. One of the issues in that case was whether a Federal District Court could issue a warrant authorizing the use of a pen register.² The

Additionally, we note, without deciding, that if a consenting party carries a camera on her person, the seizure which occurs might not be subject to the warrant requirement (cf. *United States v. White, supra*). This issue is not before us, however, because the camera used in this case was planted in defendant's office pursuant to a court-authorized entry of the building.

2. The Supreme Court described a pen register as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed" (*United States v.*

1483 court determined that rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by these devices, and also noted that in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, the court had held that rule 41 was sufficiently flexible to include the power to authorize the seizure of conversations. We believe that the similarity in the wording of rule 41 and CPL article 690 is sufficient to permit analogy. Accordingly, we conclude that the court in the instant case was authorized under CPL article 690 to issue a warrant for the seizure of intangible visual images in defendant's office.

[8] Defendant also contends that even if such a warrant is authorized under the CPL, the warrant in this case must nevertheless fall because it did not comply with the provision of title III of the Federal Omnibus Crime Control and Safe Streets Act of 1968 (U.S.Code, tit. 18, §§ 2510-2520). This is based upon the assumptions that title III applies to the area of visual electronic surveillance and that this provision pre-empts State law. Although we have previously held that title III does indeed pre-empt State law in the area of electronic surveillance (*People v. Shapiro*, 50 N.Y.2d 747, 431 N.Y.S.2d 422, 409 N.E.2d 897), this fact is unavailing in the present case, since title III does not apply to the field of video electronic surveillance and indeed, does not prohibit the type of surveillance here employed.³

Title III, also often referred to as the Federal wiretapping statute, prescribes the

New York Tel. Co., 434 U.S. 159, 161, n. 1, 98 S.Ct. 364, 366, n. 1, 54 L.Ed.2d 376, *supra*).

3. Title III specifies that an eavesdropping warrant may issue only for certain specified crimes, namely "murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in narcotic drugs, marihuana or other dangerous drugs, or other crimes dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing . . . interception, or any conspiracy to commit any of the foregoing offenses." (U.S. Code, tit. 18, § 2516, subd. [2]). In *People v. Shapiro* (*supra*) we held that allegations of prostitution and sexual abuse predicated upon the inability of

procedure for securing judicial authority to intercept wire or oral communications in the investigation of specified serious offenses. Similar to the provision of CPL article 700, which was drafted to conform to the provisions of the Federal act (see Denzer, Practice Commentary, McKinney's Cons Laws of NY, Book 11A, CPL art. 700, p. 243), title III deals only in the aural acquisition of the contents of any wire or oral communication. As the language and legislative history of that statute makes clear, it was never intended to address the use of video surveillance equipment (see Carr, *Electronic Surveillance*, § 3.08, p. 124; Senate Report No. 1097, 90th Cong, 2d Sess, U.S. Code Cong. & Admin. News, 1968, p. 2112, 2178).⁴

[9] Defendant makes one final argument concerning the video tape evidence which deserves attention. He maintains that the use of visual surveillance is so intrusive that any act of this nature should be deemed unreasonable per se under the Fourth Amendment. While we agree with defendant's concern over the high degree of intrusiveness that is inherent in this form of surveillance, we cannot agree that such activities are per se unreasonable and must be prohibited under all circumstances. Certainly the Orwellian overtones involved in this activity demand that close scrutiny be given to any application for a warrant permitting video electronic surveillance. Nevertheless, the Fourth Amendment does not mandate an absolute ban on video surveillance any more than it mandates a total

the victim to consent by reason of age did not fall within this list of enumerated crimes. On the basis of our holding in *Shapiro*, defendant argues that the Federal act also precludes electronic surveillance in cases involving only the crime of sexual abuse committed against a victim who is incapable of consent by reason of physical helplessness.

4. Specifically, the Senate report provides as follows: "Paragraph (4) defines 'intercept' to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation".

proscription on electronic eavesdropping. Indeed, there may be situations such as the present one where the intrusion resulting from such surveillance is warranted because of the State's high interest in gathering evidence of criminality and its inability to achieve this goal through less intrusive means.

Although there are at present no significant statutory limitations in the field of video electronic surveillance, we are not completely without guidance in this area. In *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 and *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, *supra*, both of which predated the advent of title III in the area of electronic eavesdropping, the Supreme Court set forth the minimum constitutional standards governing the use of aural electronic surveillance. Because of the substantial similarities between this form of surveillance and the video electronic surveillance which took place in this case, we believe that the standards announced in *Berger* and *Katz* are applicable with equal force to the present situation. And, contrary to defendant's assertions, we believe that these constitutional standards were here satisfied.

[10] The first requirement for a warrant authorizing video electronic surveillance, as with any warrant, is that there be a showing of probable cause. In situations involving this form of search, there must be probable cause to believe that a particularly described person is committing, has committed, or is about to commit a crime, probable cause to believe that the place where the activity is to be intercepted is being used or is about to be used in connection with the commission of the crime by that described person, and also probable cause to believe that a particular activity related to that crime will be observed through the use of video electronic surveillance (see *Berger v. New York*, *supra*; cf. CPL 700.15, subds. 2, 3, 5). Such probable cause was clearly established by the affidavit offered by the District Attorney in support of his application for a warrant, which fully set forth the facts leading up to the Beineix incident.

The Constitution also requires particularization in the warrant. Specifically, the Fourth Amendment commands that the warrant must particularly describe "the place to be searched, and the things to be seized". In the area of video electronic surveillance, as in the area of electronic eavesdropping, the particularization requirement includes specification of the crime under investigation, specification of the type of activity sought to be captured by the camera and also specification of the person expected to be seen performing the activity. The obvious purpose of this requirement is to limit the discretion of the officers in executing the search. Here, all of these requirements were satisfied. Although the warrant did not specify the particular room in which the camera was to be placed, the affidavit, which was incorporated in the warrant, did specify that the camera was to be placed in defendant's dental office and was to focus upon the dental chair in which consenting patients would be seated. While defendant apparently had two treatment rooms, we nevertheless conclude that the limitation upon the place to be searched was sufficiently specific to obviate the danger of a general rummaging for evidence or a search of impermissibly broad scope (see *Coolidge v. New Hampshire*, 403 U.S. 443, 91 S.Ct. 2022, 29 L.Ed.2d 564).

Minimization is also necessary for a warrant authorizing video electronic surveillance. In *Berger*, the court expressed concern that conversations of persons coming into an area covered by an eavesdropping device might be unnecessarily and indiscriminately seized without regard to their connection with the crime under investigation. This concern is equally compelling when visual surveillance is employed. The warrant in this case explicitly provided, however, that the surveillance be conducted in such a way as "to minimize the recording of activities not related to the [specified] crimes". Moreover, the incorporated affidavit expressly limited the view of the camera to the dental chair in defendant's office and specified that the device would be

52 N.Y.2d 657

PEOPLE v. DITTA

855

Cite as, Ct.App., 439 N.Y.S.2d 855

turned on only when consenting females were in the treatment room. These limitations were sufficient to ensure that the surveillance would be confined to the observation of the activities for which the warrant was issued.

Finally, before a warrant authorizing unconsented video electronic surveillance may issue, it must be established that there are no less intrusive means for obtaining the needed evidence. Since electronic surveillance of any kind is necessarily surreptitious and constitutes an extensive invasion of the individual's privacy, it may only be permitted where normal investigative procedures had been tried and had failed or are demonstrably unlikely to succeed. Defendant contends that such a showing could not be made in this case, but the facts do not bear out his contention. Before applying for the warrant the police had questioned defendant about one of the complaints of sexual abuse, had equipped two of the female complainants with hidden recorders and transmitters in an attempt to elicit admissions from defendant, and had tapped the telephone of a complainant who had received repeated calls from defendant.

Furthermore, the use of a police decoy without the protection of visual surveillance would not have produced the needed evidence in this case, since the decoy, of necessity, would have been heavily sedated and might not have been able to relate what transpired. Under these circumstances it cannot be said, despite defendant's protestations to the contrary, that the police failed to make a sufficient showing of necessity before obtaining the warrant.

As we have stressed, the constitutional requirements outlined for eavesdropping in *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040, *supra*, and *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576, *supra* are equally applicable to the area of video electronic surveillance. While we have discussed several of these requirements in the instant case our opinion should not be construed as an inventory of each of the necessary elements for such a warrant. The degree of intrusiveness inherent in video electronic surveillance de-

mands unswerving adherence to each of the limitations placed upon the use of this device. Moreover, because the use of this investigative technique poses a threat to the privacy of citizens, legislative scrutiny of the field and the enactment of specific guidelines would appear to be in order.

We have considered defendant's remaining contentions and conclude that they are without merit.

Accordingly, the order of the Appellate Division, 73 A.D.2d 136, 425 N.Y.S.2d 315 should be affirmed.

COOKE, C. J., and JASEN, JONES, WACHTLER, FUCHSBERG and MEYER, JJ., concur.

Order affirmed.



422 N.E.2d 515

52 N.Y.2d 657

The PEOPLE of the State of New York, Respondent,

v.

John DITTA, Appellant.

Court of Appeals of New York.

May 12, 1981.

Defendant was convicted before the Supreme Court, Queens County, Eugene Sharpe, J., of sexual abuse in the first degree, unlawful imprisonment in the second degree, criminal possession of a weapon in the fourth degree, endangering the welfare of a child, and menacing, and he appealed. The Supreme Court, Appellate Division, 77 A.D.2d 604, 429 N.Y.S.2d 979, affirmed. Permission to appeal was granted. The Court of Appeals, Cooke, C. J., held that one may be convicted of sexual abuse in the first degree where he compels another per-

they wish to accept as a debtor and owner of the security, and to reappraise the desirability of the loan originally made from the standpoint of the then value and condition of the security covered and the interest rate obtainable in the current money market. The Kennedy's sale of the mortgaged premises gave Hudson the option to make such decisions and reappraisals, and as a result it has elected to declare the mortgage due and payable. The acceleration clause was one which the parties to the mortgage agreed to in a fair and legal contract, and does not constitute a forfeiture or a penalty (*Graf v. Hope Building Corp.*, 254 N.Y. 1, 171 N.E. 384; *Albertina Realty Co. v. Rosbro Realty Corp.*, 258 N.Y. 472, 180 N.E. 176." (63 Misc.2d 863, 866, 313 N.Y.S.2d 804, 808.)

[1] Clearly, the circumstances in a given case might be such as to restrict or restrain the mortgagee's right to accelerate under a due-on-sale provision such as that found in this case. Since the issue of mortgage foreclosure falls within the Court's equity jurisdiction, the court sitting in equity may refuse to enforce the clause when acceleration of the due date would effect an unconscionable or unfair result. See, e.g., *Loughery v. Catalano*, 117 Misc. 393, 191 N.Y.S. 436; *Scheible v. Leinen*, 67 Misc.2d 457, 324 N.Y.S.2d 197; *Clark v. Lachenmeier* (1970, Fla.App.), 237 So.2d 583; *Gibraltar Finance Corp. v. Rouse* (1933), 145 Or. 89, 25 P.2d 559; *Mutual Federal S. & L. Assn. v. Wisc. Wire Works* (1973), 58 Wis.2d 99, 205 N.W.2d 762, 69 A.L.R.3rd 702; *Mutual Federal S. & L. Assn. v. American Med. Services, Inc.* (1974), 66 Wis.2d 210, 223 N.W.2d 921.

There are no facts set forth which require such a result in this case. The only allegation in the complaint bearing upon defendant's reasons or motives for refusing to consent to the sale is to the effect that defendant's Pennsylvania agent had a favored customer who wished to purchase the property at a price lower than that offered by plaintiff's purchaser. This allegation naturally carries with it the implication

that defendant was not dealing in good faith and resorted to the due-on-sale clause so as to unconscionably and inequitably interfere with plaintiff's right of free alienation. However, plaintiff's allegations in this regard are conclusory and his papers on the motion fail to come forward with any supporting evidentiary detail. Plaintiff's assertion that defendant's Pennsylvania agent gave assurances that defendant would approve the sale if made to the favored customer is of no particular significance as it appears that similar assurances were made with respect to the proposed sale to plaintiff's preferred purchaser. In any event, it is far from clear whether the Pennsylvania concern was acting herein as defendant's agent, as such, with authority to modify or terminate defendant's mortgage agreements with plaintiff or rather as a mere means of communication between the parties. No proof has been submitted that the Pennsylvania entity was authorized in writing to act on defendant's behalf regarding a waiver of defendant's right to accelerate in case of sale (General Obligations Law, § 5-1111).

Although the "due-on" device is frequently employed, the appellate courts in our state have not as yet considered its legal effect. Perhaps, as suggested by Professor Leon Wein (*Due On Sale in New York*, 49 N.Y. State Bar Journal 203 [1977] at p. 242: " * * * the legislature might devise a set of standards to restructure commercial morality as it is associated with the extension of mortgage credit".

[2] Accordingly, the motion for summary judgment is granted to the extent of directing judgment in favor of the defendant declaring: (1) that the clause in question is not void and unenforceable according to its terms; (2) that defendant's refusal to consent to the sale of the mortgaged property to a financially responsible purchaser does not constitute, in and of itself, an unconscionable or inequitable exercise of its option to accelerate the balance due pursuant to the due-on-sale clause, which option is accordingly entitled to judicial enforcement. The first and fourth causes of action are dismissed.

PEOPLE v. TEICHER

587

Cite as 395 N.Y.S.2d 567

90 Misc.2d 638

The PEOPLE of the State of New York

v.

Marvin TEICHER, Defendant.

Supreme Court, New York County,

Part 106.

June 2, 1977.

*St. Ann
Victim consent
(3) Partially
minimization*

Dentist who was charged with sexual abuse of patients filed a motion to controvert the warrant to secretly place a camera in his dental offices to videotape the events of patients' visits, and to suppress the film obtained from use at the trial. The Supreme Court, Robert M. Haft, J., held that: (1) the installation of video surveillance equipment and monitoring of the dentist's activities constituted a "search and seizure" within scope of the Fourth Amendment; (2) a visual observation may fall within the scope of "property" subject to seizure if it constitutes evidence or tends to demonstrate that an offense was committed; (3) a seizure will be legal if it is derived pursuant to a proper warrant issued by a neutral magistrate; (4) the New York statutes authorize issuance of a warrant to videotape evidence and, in any event, the Supreme Court, in exercise of its inherent powers had authority to issue such a warrant; (5) the issuing court had ample reason to be satisfied with the personal credibility of the named informants and reliability of their information so that it had probable cause for issuing the warrant, and (5) the application and resulting order stated with sufficient particularity the place where videotape camera was to be installed, the area and conduct which were to be observed, and how long such observations were to continue.

Defendant's motion denied.

1. Searches and Seizures ¶7(1)

The installation of video surveillance equipment and monitoring dentist's alleged sexual abuse of patients in his office was a "search and seizure" within scope of the Fourth Amendment. U.S.C.A. Const. Amend. 4.

See publication Words and Phrases for other judicial constructions and definitions.

2. Telecommunications ¶494

Title III of the Omnibus Crime Control Act of 1968 and its progeny, the state wiretapping statutes, did not encompass videotaping or any means of electronic visual surveillance. 18 U.S.C.A. §§ 2510-2520; CPL 690.05 et seq., 700.05 et seq.

3. Searches and Seizures ¶2.4

Warrants for videotaping must comply with the guidelines promulgated by the Supreme Court of the United States, since videotaping captures conversations by means of electronic surveillance; compliance would be accomplished if statutory requirements of New York eavesdropping statute were met. CPL 700.05 et seq.

4. Searches and Seizures ¶3.1

Since videotaping encompasses two components, visual surveillance and aural surveillance, the statute which deals exclusively with aural communication cannot alone serve as predicate for issuing a court order to videotape, and hence search warrant statute must be examined to determine if the seizure of visual images is within the ambit of its search warrant provisions. CPL 690.05, subd. 2, 690.10, subd. 4, 700.05 et seq.

5. Searches and Seizures ¶7(10)

A visual observation may fall within the scope of "property" subject to seizure if it constitutes evidence or tends to demonstrate that an offense was committed. CPL 690.10, subd. 4.

See publication Words and Phrases for other judicial constructions and definitions.

6. Searches and Seizures ¶3.1

The seizure that results from obtaining visual observation of a crime in progress in a private place will be legal if it is derived pursuant to a proper warrant issued by a neutral magistrate. CPL 690.05 et seq.

7. Searches and Seizures ¶3.4

The Supreme Court has inherent power to issue a videotape order to assist in criminal investigation.

8. Criminal Law \Leftrightarrow 207(3)Searches and Seizures \Leftrightarrow 3.4

The New York Supreme Court's jurisdiction and power are coextensive with authority exercised in 1776 by the Kings Bench and Court of Chancery in England, as well as the Supreme Court of the colony of New York, which powers include the right to assist in investigation of criminal activity by issuing search and arrest warrants. Judiciary Law \S 140-b.

9. Searches and Seizures \Leftrightarrow 3.4

CPL Articles 690 and 700, read together, authorize the issuance of a warrant to videotape evidence in assisting criminal investigations and, in any event, the Supreme Court, in exercise of its inherent power, had authority to issue such a warrant so long as it conformed to the Fourth Amendment requirements of probable cause, particularity, and limitation of scope. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

10. Searches and Seizures \Leftrightarrow 3.6(2)

Where application for warrant to secretly place a camera in dentist's offices to videotape alleged sexual abuses of patients consisted of affidavit from detective, the county district attorney and assistant district attorney based on information supplied by patients whose accounts were somewhat corroborated, the issuing court had ample reason to be satisfied with both the personal credibility of the named informants and the reliability of their information so that warrant was based on probable cause. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

11. Searches and Seizures \Leftrightarrow 3.7

A search warrant must state with particularity the persons or places authorized to be searched and the things to be seized so that an executing officer can reasonably identify them; to protect one's right of privacy from arbitrary governmental intrusions, nothing should be left to discretion of the searcher in executing the warrant, but hypertechnical accuracy and completeness of description need not be attained; rather, the warrant must be viewed from the

standpoint of common sense. U.S.C.A. Const. Amend. 4.

12. Searches and Seizures \Leftrightarrow 3.7

The descriptions in search warrant and the accompanying affidavits should be sufficiently definite to enable the searcher to identify the persons, places, or things that the neutral magistrate has previously determined should be searched or seized. U.S.C.A.Const. Amend. 4.

13. Searches and Seizures \Leftrightarrow 3.7

Where warrant to secretly place a camera in dental offices provided that camera should remain in stationary position and to point only towards dental chair in which consenting females would be seated and that equipment would be turned on only when consenting females had appointments in order to visually capture dentist's activities which were expected to be similar to that which had reportedly occurred in the past with three other patients, the instructions for officers conducting the search appeared to be sufficiently particularized so that warrant could not be struck down on grounds of lack of particularity. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

14. Searches and Seizures \Leftrightarrow 3.7

Technical errors in a portion of description of premises to be searched will not invalidate a warrant if the premises can be identified with reasonable effort and there is no reasonable probability that a search may be made of premises other than those intended to be searched under the warrant. U.S.C.A.Const. Amend. 4.

15. Criminal Law \Leftrightarrow 394.4(7)

Dentist prosecuted, for sexual abuse of patients, was not entitled to suppression of film obtained from use of videotape on ground that the videotape camera installed pursuant to warrant was not placed in the first examining room on the left, as stated in affidavit, where order required visual surveillance equipment to be installed at a certain address on the first floor, where defendant had his offices, where he engaged in practice of dentistry, and where

PEOPLE v. TEICHER

589

Cite as 395 N.Y.S.2d 587

his patients received treatment, and if the videotaping occurred in the "second" instead of "first" room, there was no dispute that the defendant did treat the undercover policewoman in the room in which the videotaping occurred. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

16. Criminal Law ⇐394.4(6)

Dentist, prosecuted for sexual abuse of patients, was not entitled to suppression of film obtained from videotape camera on ground that specific acts which the videotape equipment intended to capture on film were not delineated with sufficient particularity in the warrant, where affidavit set forth in minute detail the acts allegedly perpetrated against first three complaining patients and sought evidence of similar acts that might be committed against undercover police agent or other patients cooperating with the authorities; the prosecution was not required to attempt to read the mind of the defendant and state explicitly each and every act it believed he would commit. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

17. Searches and Seizures ⇐3.6(1)

A warrant to secretly place a camera in dentist's offices to videotape alleged sexual abuses of patients was not invalid for failure to provide adequately for minimization, where affidavit indicated that monitoring would occur only when consenting females were patients, and it was apparent from the use of plural "consenting females" that district attorney was contemplating the use of more than one undercover or cooperative patient within the 30-day period and had not made any decision as to the number. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A. Const. Amend. 4.

18. Criminal Law ⇐394.6(2)

Dentist, prosecuted for sexual abuse of patients, was not entitled to suppression of film obtained from use of videotape camera on ground that extraordinary use of videotape was unwarranted because other investigative tools were available to the govern-

1. A survey of other jurisdictions reveals that many courts have considered the introduction

ment in pursuit of its investigation, where use of consensual aural recording proved to be of minimal assistance, use of undercover agent alone could yield little in the way of additional evidence, particularly during period when agent was expected to be rendered unconscious or semiconscious, and principal reason for use of videotape was to obtain information during period when drugs had taken their full effect, since none of the earlier victims were able to relate what sexual activities had taken place before their return to consciousness. CPL 690.05 et seq., 700.05 et seq.; U.S.C.A.Const. Amend. 4.

Robert M. Morgenthau, Dist. Atty. of New York County, by Linda Fairstein, Asst. Dist. Atty., for the People.

Rothblatt, Rothblatt, Seijas & Peskin, by Steven Peskin, New York City, for the defendant.

ROBERT M. HAFT, Judge.

Defendant, a practicing dentist in the Chelsea district in Manhattan, is charged with three counts of sexual abuse in the first degree, arising from his alleged sexual touching and fondling of three of his female patients after he had injected certain drugs (sodium secobarbital and valium) for the purpose of dental extractions. It is the People's contention that the drugs rendered the patients "physically helpless" and thus incapable of consenting to the sexual contact.

The last of these patients was an undercover policewoman and in conjunction with arranging her appointment with defendant for the extraction of a wisdom tooth, the People applied for and obtained a warrant from a Justice of the Supreme Court to secretly place a camera in defendant's dental offices to videotape the events of the visit. Defendant's motion to controvert this warrant and suppress the film obtained from use at the trial presents several novel issues of first impression.¹

of videotape evidence, but none have done so in the context of evidence acquired by court

Defendant contends that suppression is required. He claims that the installation of video surveillance equipment and the monitoring and taping of his activities within his office was a search and seizure within the meaning of the Fourth Amendment, and that this search and seizure were unreasonable for the following reasons:

1. There is no statutory authority in this State for the issuance of an order to videotape.

2. The order was improper because the accompanying affidavits are based on unsupported hearsay and therefore fail to establish probable cause.

3. The order was invalid, in any event, because it did not conform to the minimal constitutional standards established for electronic eavesdropping by not specifying: (a) the precise location where the camera was to be installed, (b) the precise activities and area to be observed, (c) the manner in which minimization was to be accomplished and (d) a reasonable limitation during which surveillance was to continue.

4. The order was improvidently granted since normal investigative procedures had not been exhausted before the radical technique of videotaping was employed.

The Fourth Amendment provides:

"The right of the people to be secure in their persons, houses, papers, and effects,

order of transactions in a person's private office. (See *e. g.*, *State v. Hewett*, 86 Wash.2d 487, 545 P.2d 1201 [Sup.Ct.Wash.1976], videotaping of a deposition; *Hendricks v. Swenson*, 456 F.2d 503 [8th Cir. 1972] and *State v. Lusk*, 452 S.W.2d 219 [Mo.1970], videotaping of confessions, *People v. Heading*, 39 Mich.App. 126, 197 N.W.2d 325 [Ct. of App. Mich.1972], videotaping of a lineup; *Mikus v. United States*, 433 F.2d 719 [2d Cir. 1970], videotaping of a bank robbery; *Avery v. State*, 15 Md.App. 520, 292 A.2d 728 [Ct. of Spec. App.Md.], *app. dsmd.* 410 U.S. 977, 93 S.Ct. 1499, 36 L.Ed.2d 173 [1972], videotaping in private home with consent of the owner of defendant engaging in assault).

Other than the use of videotaping trials, *e. g.* "Note, Videotaped Trials, a Practical Evaluation and Legal Analysis," 26 Stanford L.Rev. 619 (1974), few articles deal with videotaping as a method of obtaining evidence (see "Criminal Prosecution Videotape Film," 60 A.L.R.3d

against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized."

The Supreme Court in *Katz v. United States*, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), held that whether the police have conducted a search within the meaning of the Fourth Amendment does not depend upon a property right in the invaded place, but rather upon whether the area is one in which there is reasonable expectation of freedom from governmental intrusion. Traditionally, a doctor's office has been so regarded (*Mancusi v. DeForte*, 392 U.S. 364, 88 S.Ct. 2120, 20 L.Ed.2d 1154 [1968]; *People v. Abruzzi*, 52 A.D.2d 499, 385 N.Y.S.2d 94 [2nd Dept. 1976], *aff'd* 42 N.Y.2d 813, 396 N.Y.S.2d 649, 364 N.E.2d 1342 (1977).

Further, courts have employed the *Katz* expectation of privacy rationale to provide security from nonjudicially sanctioned visual surveillance of private places and actions (*People v. Abruzzi, supra*).²

[1] There is no doubt that the installation of video surveillance equipment and the monitoring of Dr. Teicher's activities in his office was, indeed, a search and seizure within the scope of the Fourth Amendment.

333; Ward, "Judicial Administration—Technological Advances—Use of Videotape in the Courtroom and the Stationhouse," 20 DePaul L.Rev. 924 (1971); Hedges, "Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother?," 3 Hastings Const. L.Q. 261 (1976)).

2. See *People v. Terrell*, 53 Misc.2d 32, 277 N.Y.S.2d 926 [Sup.Ct. Bronx Co., 1967], *aff'd* 30 A.D.2d 644, 291 N.Y.S.2d 1002 [1st Dept. 1968]; *People v. Diaz*, 85 Misc.2d 41, 376 N.Y.S.2d 849 [Cr.Ct.N.Y.Co.1975]; *Jacobs v. Superior Ct. of Stanislaus County*, 36 Cal.App.3d 489, 111 Cal. Rptr. 449 [Ct. of App., 5th Dist. 1973]; *State v. Person*, 34 Ohio Misc. 97, 298 N.E.2d 922 [Mun.Ct. Toledo 1973]; *State v. Di Bartolo*, 276 So.2d 291 [Sup.Ct.La.1973]; *cf.* cases predating *Katz*, decided on the same basis, *California v. Hurst*, 325 F.2d 891 [9th Cir. 1963] and *Brock v. United States*, 223 F.2d 681 [5th Cir. 1955].

PEOPLE v. TEICHER

591

Cite as 395 N.Y.S.2d 587

The defendant argues that issuance of the instant warrant was entirely without statutory authority. It is his position that a warrant may issue subject only to a specific statute and that search and seizure by videotape is not provided by either CPL Article 690 or Article 700 (the New York statutes dealing with the issuance of warrants).

The order and underlying affidavits submitted to the issuing court do not specifically state that this warrant was issued pursuant to Article 690 or 700 or both. However, the application for the warrant clearly indicates an effort to comply with the stricter and more particularized formulations of CPL Article 700, the eavesdropping statute, as well as to show probable cause for its issuance pursuant to Article 690.

CPL section 700.15 states as follows:

"An eavesdropping warrant may issue only:

'1. Upon an appropriate application made in conformity with this article; and

'2. Upon probable cause to believe that a particularly described person is committing, has committed, or is about to commit a particular designated offense; and

'3. Upon probable cause to believe that particular communications concerning such offense will be obtained through eavesdropping; and

'4. Upon a showing that normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or to be too dangerous to employ; and

'5. Upon probable cause to believe that the facilities from which, or the place where the communications are to be intercepted, are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such persons.'"

[2] The process of videotaping consists of the simultaneous use of a camera and

3. Videotaping was invented by Ampex Corp. of Redwood City, California, in 1956. It received widespread acceptance in the business community starting in 1963 with the advent of smaller

microphone to convert light energy and sound waves into electronic impulses, which impulses are stored on magnetic tape that can be played back to recreate the audio and visual scene so recorded (Ward, "Judicial Administration—Technological Advances—Use of Videotape in the Courtroom and Stationhouse," 20 DePaul L.Rev. 924 (1971)). Thus, videotaping does appear to be a device for "mechanically overhearing a conversation" as that term is defined in Penal Law, section 250.00(2) and used in Article 700 of the CPL. It does, however, add a new dimension of visual pickup to the normal means of eavesdropping, which focuses solely on capturing aural evidence. The courts, the legislature, and commentators agree that Title III of the Omnibus Crime Control Act of 1968, 18 U.S.C. §§ 2510–2520 and its progeny, the state wiretapping statutes, did not encompass videotaping or any means of electronic visual surveillance (see *Avery v. State*, *supra*, 15 Md.App. 520, 292 A.2d 728 [Ct. of Spec.App. Md.], *app. dsmd.* 410 U.S. 977, 93 S.Ct. 1499, 36 L.Ed.2d 173 [1972], Senate Report No. 1097, 90 Cong.2d Sess. [1968] 1968 *U.S. Code Congressional and Administrative News*, p. 2153 et seq.; Hodges, "Electronic Visual Surveillance and the Fourth Amendment: The New Arrival of Big Brother?", 3 *Hastings Const.L.Q.* 261 [1976]). Our Legislature in drafting section 700.15 seemed not to have considered it.

[3] When, in 1968, most eavesdropping statutes were redrafted to comport with the requirements set forth by the Supreme Court in *Katz v. United States*, *supra* and *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967) (Senate Report No. 1097 *supra*; Practice Commentary, McKinney's Cons.Laws of New York, CPL, Book 11A, p. 243), videotaping in industry, government and education was not widespread though it had been in use since 1956.³ Certainly, warrants for videotaping must comply with the guidelines of *Katz*

portable models of closed circuit systems. (See Ward, Comment Judicial Administration—Technological Advances. *supra*.)

and *Berger*, since videotaping does capture conversations by means of electronic surveillance. Compliance would be accomplished if the statutory requirements of Article 700 are met. (See *United States v. Cirillo*, 499 F.2d 872 [2d Cir. 1974], upholding the constitutionality of the CPL eavesdropping provisions.) Consequently, although the warrant ordered here was not explicitly issued pursuant to CPL Article 700, it must at least meet the standards imposed by that statute to pass muster.

[4] Since videotaping encompasses two components—visual surveillance and aural surveillance—Article 700 of the CPL which deals exclusively with aural communication cannot alone serve as predicate for issuing a court order to videotape. We must, therefore, examine Article 690 to determine if the seizure of visual images is within the ambit of its search warrant provisions.

Section 690.05(2) of the CPL, in pertinent part, provides:

“A search warrant is a court order and process directing a police officer to conduct a search of designated premises, . . . or of a designated person, for the purpose of seizing designated property or kinds of property”

[5] “Property” subject to seizure is defined in section 690.10(4) to include property which “constitutes evidence or tends to demonstrate that an offense was committed . . . that a particular person participated in the commission of an offense.” Thus, a visual observation may fall within the scope of property subject to be seized if it constitutes evidence or tends to demonstrate that an offense was committed.

[6] Courts that have had occasion to consider the seizure that results from obtaining visual observations of a crime in progress in a private place, all indicate that the seizure will be legal if it is derived pursuant to a proper warrant issued by a neutral magistrate (*People v. Abruzzi*, 52 A.D.2d 499, 385 N.Y.S.2d 94 (2d Dept. 1976), *affd.*, 42 N.Y.2d 813, 396 N.Y.S.2d 649, 364 N.E.2d 1342, 1977) and other cases cited *supra*, page 503, 385 N.Y.S.2d page 97, n.2.

In *Abruzzi*, the Appellate Division, Second Department, found that visual observations by police in the course of committing a trespass on a doctor's property without a warrant, after having received complaints of sexual misconduct from the doctor's patients, was a search and seizure in violation of the Fourth Amendment. Implicit in this ruling, however, is the fact that a search warrant under CPL Article 690 could have issued to permit the police to make observations from a private place.

It thus appears that the issuance of a warrant to obtain both visual and aural surveillance must meet the tests of both Articles 690 and 700 of the CPL. However, neither article explicitly contemplates the means employed herein—namely videotape—but both read together would seem to encompass this situation. Whether or not Articles 690 and 700 explicitly authorize videotaping, the People urge an alternate theory: the inherent power of the Supreme Court to assist in criminal investigations and to issue the necessary judicial process as authority for the promulgation of a warrant to videotape. It is contended that the legislature in specifying the procedures for the issuance of search warrants and electronic eavesdropping warrants had not sought to limit the court's inherent power and that nothing precludes the issuance of a court order for videotaping so long as the order conforms to the dictates of the Fourth Amendment.

[7, 8] This court agrees that there is inherent power to issue a videotape order. The Supreme Court in *Katz* and *Berger*, *supra*, permitted electronic eavesdropping pursuant to warrant under certain strict minimal standards. It did not mandate that eavesdropping could only be performed pursuant to statutory authority. Indeed, historically, trial courts throughout the country have exercised their inherent right to issue search warrants. In New York, this power dates back to pre-revolutionary days (*Hamlin & Baker*, Supreme Court of the Judicature of the Province of New York, 1691-1704, pp. 68-77). The New York Supreme Court's jurisdiction and pow-

PEOPLE v. TEICHER

593

Cite as 393 N.Y.S.2d 567

er are coextensive with the authority exercised in 1776 by the Kings Bench and Court of Chancery in England, as well as the Supreme Court of the Colony of New York (Judiciary Law, § 140-b; *Matter of Steinway*, 159 N.Y. 250, 258, 53 N.E. 1103, 1105 [1899]). These powers include the right to assist in investigation of criminal activity by issuing search and arrest warrants and those warrants were not issued pursuant to explicit statutory authority (see 1 M. Hale, *The History of the Pleas of the Crown*, 577-78 [1st Amer. ed. 1847]; 2 M. Hale, *id.* 113-14; 149-150).

[9] Thus, this court holds that CPL Articles 690 and 700, read together, authorize the issuance of a warrant to videotape evidence and, in any event, the Supreme Court, in the exercise of its inherent powers, had the authority to issue such a warrant so long as it conformed to the Fourth Amendment requirements of probable cause, particularity, and limitation of scope. The defendant has additionally challenged the videotape warrant on each of those grounds which must now be severally considered.

The application for the warrant consists of affidavits from Detective Inge Macri of the Manhattan Sex Crimes Squad of the New York City Police Department, New York County District Attorney Robert M. Morgenthau and Assistant District Attorney Leslie Snyder. The Macri affidavit outlines the facts underlying the application based upon the statements of three young female patients alleged to be victims of the defendant's sexual abuse.⁴ The other two affidavits refer, in turn, to the Macri affidavit and opine that there are no other investigative procedures which were not tried which might prove successful.

Defendant argues that a finding of probable cause may not be made solely on hearsay allegations unless there is substantial basis for crediting that evidence. He maintains that if the court were to apply the established *Aguilar-Spinelli* analysis to Det.

Macri's affidavit, it would have to controvert the warrant, because the reliability of the informants and their information were not established.

In *Aguilar v. Texas*, 378 U.S. 108, 84 S.Ct. 1509, 12 L.Ed.2d 723 (1964), the Supreme Court established a two-pronged test to determine the reliability of hearsay allegations. The first prong, the veracity test, is directed at the trustworthiness of the person supplying the information and requires the affiant to set forth the reasons which led him to conclude that the informer was credible or that his information was reliable. The second prong, or basis of knowledge test, concerns the trustworthiness of the information and requires that the affiant state the facts and circumstances relied on by the informer in reaching his conclusions. In *Spinelli v. United States*, 393 U.S. 410, 89 S.Ct. 584, 21 L.Ed.2d 637 (1969), the Supreme Court supplemented *Aguilar* by suggesting new methods of satisfying the two-pronged analysis. Thus, the Supreme Court found that as to the first prong—the veracity test—either personal credibility or informational reliability may be satisfied by independent verification of the hearsay. In *United States v. Ventresca*, 380 U.S. 102, 85 S.Ct. 741, 13 L.Ed.2d 684 (1965), followed in *Spinelli*, the court held that the second prong might be satisfied absent a statement recounting the manner in which the information was gathered, by providing so detailed a description of the suspect's criminal activity as to constitute self-verification. The New York Court of Appeals has taken a parallel tack and permitted additional and similar means of meeting the *Aguilar* guidelines. (See *People v. Hanlon*, 36 N.Y.2d 549, 557, 369 N.Y.S.2d 677, 330 N.E.2d 631 [1975]).

The reliability of the information furnished the affiant is usually established by a statement that the unnamed "informer" has in the past furnished information leading to arrest and conviction of others. (See *People v. Slaughter*, 37 N.Y.2d 596, 376

4. Two of these three patients testified before the Grand Jury, reaffirming their statements to Det. Macri.

N.Y.S.2d 114, 338 N.E.2d 622 [1975]; *People v. Hendricks*, 25 N.Y.2d 129, 303 N.Y.S.2d 33, 250 N.E.2d 323 [1969].) But such is not the case here. The three informants are named citizens who claimed to be victims of the crimes alleged against the defendant.

In *People v. Wheatman*, 29 N.Y.2d 337, 345, 327 N.Y.S.2d 643, 647, 277 N.E.2d 662, 665 (1971), *cert. den. sub. nom. Marcus v. New York*, 409 U.S. 1027, 93 S.Ct. 460, 34 L.Ed.2d 321 the Court of Appeals indicated that a magistrate may rely on information where two or more informants tend to confirm the information each gave. In this case, each victim gave a very detailed account of defendant's abusive actions. Defendant's pattern of conduct as to each victim was quite similar. Little variation can be found in the accounts. Thus, each victim's account tended to corroborate the others and served to negate the likelihood that the complainants were suffering from drug-induced delusions or hallucinations or that their information based on first-hand knowledge was unreliable.

Moreover, courts have traditionally viewed named citizen-informants in a different light from undisclosed informers, giving the former much greater credence. *People v. Hicks*, 38 N.Y.2d 90, 378 N.Y.S.2d 660, 341 N.E.2d 227 (1975).⁵ In this case, the detailed version of any one of the victim-informants would have provided sufficient probable cause for defendant's arrest.⁶ The fact that they might be subject to criminal or civil action for false arrest or malicious prosecution would be an additional basis for assuming a lack of fabrication. (*Adams v. Williams*, 407 U.S. 143, 92 S.Ct. 1921, 32 L.Ed.2d 612 [1972].)

Furthermore, there was some corroboration of their accounts. The defendant ad-

mitted to Det. Macri administering drugs to the first patient although claiming one of the side effects of those drugs could be hallucinations (*Macri Aff. Par. 11A*). Following the second patient's complaint, that complainant was asked to return to defendant's office wearing a Kel recording and transmitting device which, notwithstanding much interference and inaudibility, did record defendant's admission that he had kissed her and enjoyed it: "Yes, very much, very very much, very much." (*Macri Aff., Par. 11B*.) This same patient arranged a "date" at a bar with defendant at the request of the District Attorney, which was recorded but the only significant statement by defendant was that the patient had thrown her arms around him and given him a "fat kiss" and that "it's not the first time it has happened." (*Macri Aff., Par. 11C*.) After the third patient's complaint, a tape device on her phone recorded defendant asking her for a date and expressing a desire to come to her apartment, as no one would know him there, and that he would bring his "bag of goodies" from the office on this "house call" (*Macri Aff., Par. 11F*).

[10] For the reasons indicated, the issuing court had ample reason to be satisfied with both the personal credibility of the named informants and the reliability of their information. Thus, the warrant was, indeed, based on probable cause and defendant's arguments must fail.

[11, 12] Defendant further contends that the application and the resulting order do not state with sufficient particularity the place where the videotape camera was to be installed, what area and conduct were to be observed, and how long such observations were to continue. A warrant must state with particularity the persons or

icz v. Comm., 212 Va. 730, 187 S.E.2d 144 (Sup.Ct.Va.1972).

5. Also see *State v. Kurland*, 130 N.J.Super. 110, 325 A.2d 714 (Super.Ct.N.J.1974); *People v. Hill*, 12 Cal.3d 731, 117 Cal.Rptr. 393, 528 P.2d 1 (Sup.Ct.Cal.1974); *State v. Watkins*, 228 N.W.2d 635 (Sup.Ct.S.Dak.1975); *State v. O'Bryan*, 96 Idaho 548, 531 P.2d 1193 (Sup.Ct. Ida.1975); *State v. Bluin*, 315 So.2d 749 (Sup.Ct.La.1975); *State v. Drake*, 224 N.W.2d 476 (Sup.Ct.Iowa 1974); *State v. Jones*, 110 Ariz. 546, 521 P.2d 978 (Sup.Ct.Ariz.1974); *Guzew-*

6. The People claim that fairness dictated that defendant, a professional man, with no prior criminal record, who had denied the allegations made against him, should not have been summarily arrested without the additional corroboration which the videotape was intended to provide.

PEOPLE v. TEICHER

595

Cite as 393 N.Y.S.2d 587

places authorized to be searched and the things to be seized so that an executing officer can reasonably identify them (*Steele v. United States No. 1*, 267 U.S. 498, 503, 45 S.Ct. 414, 69 L.Ed. 757 [1925]; *People v. Nieves*, 36 N.Y.2d 396, 369 N.Y.S.2d 50, 330 N.E.2d 26 [1975]). Thus, to protect one's right of privacy from arbitrary governmental intrusions, nothing should be left to the discretion of the searcher in executing the warrant (*Marron v. United States*, 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 [1927]; *People v. Nieves*, *supra*). This does not mean, however, that hypertechnical accuracy and completeness of description must be attained; rather, the warrant must be viewed from the standpoint of common sense (*United States v. Ventresca*, *supra*, 380 U.S. at 108, 85 S.Ct. 741; *People v. Hendricks*, *supra*, 25 N.Y.2d at 137, 303 N.Y.S.2d at 39, 250 N.E.2d at 327). The descriptions in the warrant and the accompanying affidavits should be sufficiently definite to enable the searcher to identify the persons, places, or things that the neutral magistrate has previously determined should be searched or seized (*People v. Nieves*, *supra*).

[13] The warrant in this case provided for the installation of a videotape recorder in defendant's offices at 167 Eighth Avenue on the first floor. The affidavit provides that "(t)he camera will remain in a stationary position and will point only towards the dental chair in which the consenting females will be seated" and "(t)he equipment will be turned on only when the consenting females have appointments" with the defendant in order to visually capture defendant's activities which were expected to be similar to that which had reportedly occurred in the past with three other patients. The instructions for the officers conducting the search appear to be sufficiently particularized and so the warrant may not be struck down on the grounds of a lack of particularity.

[14, 15] Defendant also maintains that the camera was not placed in the first examining room on the left, as stated in the Macri affidavit, but in the second room and,

therefore, the resulting search and seizure was invalid. It is clear that the order and affidavit required the visual surveillance equipment to be installed at 167 Eighth Avenue on the first floor, where defendant had his offices, where he engaged in the practice of dentistry, and where his patients received treatment. This is precisely what was done. If, indeed, the videotaping occurred in the "second" instead of the "first" room, there is no dispute that the defendant did treat the undercover police woman in the room in which the videotaping occurred. The reference to the "first" examining room in the warrant is no more than a mere technical error. Technical errors in a portion of the description of the premises to be searched will not invalidate a warrant if the premises can be identified with reasonable effort and there is no reasonable probability that a search may be made of premises other than those intended to be searched under the warrant. (*People v. Sprague*, 47 A.D.2d 510, 367 N.Y.S.2d 598 [3d Dept. 1975]; *People v. Galleges*, 80 Misc.2d 265, 362 N.Y.S.2d 1000 [Sup.Ct., Kings Co., 1975]; *People v. Mongno*, 67 Misc.2d 815, 325 N.Y.S.2d 62 [Sup.Ct., Queens Co., 1971]).

[16] Defendant's argument that the specific acts which the videotape equipment intended to capture on film are not delineated with sufficient particularity is specious. The affidavit sets forth in minute detail the acts allegedly perpetrated against the first three complaining patients and seeks evidence of similar acts that may be committed against undercover police agents or other patients cooperating with the authorities. Such a description is sufficient. The prosecution does not have to attempt to read the mind of the defendant and state explicitly each and every act it believes he will commit. It is enough to couple the evidence sought—namely, defendant's actions to be recorded—to the specific type of criminal behavior he is alleged to have committed in the past.

[17] Defendant additionally urges that the warrant fails to provide adequately for minimization; in particular, he points to the

last paragraph of the order which states that "the order shall not automatically terminate when a photographic record of the activities described herein has first been obtained but in no event shall it exceed 30 days" Defendant claims that CPL 700.30(7) mandates that a warrant must terminate upon attainment of its objective; otherwise it is overly broad and invalid. However, this warrant calls for minimization in the prior paragraph, and the affidavit indicates that monitoring would occur only when *consenting females* were patients. Furthermore, it is quite apparent from the use of the plural "consenting females" that the District Attorney was contemplating the use of more than one undercover or cooperative patient within the thirty-day period and had not made any decision as to the number. Thus, even if he were successful in obtaining evidence as to one patient, he desired the option of pursuing the matter on the ground that the defendant's conduct was a repeated ongoing crime.⁷ The continuing repetitious crime theory has been accepted in various gambling cases (see *People v. Gnozzo*, 31 N.Y.2d 134, 335 N.Y.S.2d 257, 286 N.E.2d 706 [1972]). This court finds that the warrant provided for adequate minimization and only limited intrusion.

[18] Lastly, defendant argues that the extraordinary use of videotape was unwarranted because other investigative tools were available to the government in its pursuit of this investigation. This court disagrees. The use of consensual aural recording had proved to be of minimal assistance. The use of an undercover agent alone, suggested as an alternative by defendant, could yield little in the way of additional evidence, particularly during the period when the agent was expected to be rendered unconscious or semi-conscious. The principal reason for the use of the videotape was to obtain information during the period when the drugs had taken their full effect since none of the earlier victims

7. Of course, since the defendant was actually arrested at the time of the videotaping of his encounter with the first undercover policewom-

were able to relate what sexual activities had taken place before their return to consciousness. Such activity could take place in complete silence, and the expected high level of extraneous background noise in a dentist's office rendered an electronic eavesdropping device useless. Further, the personal safety and dignity of any female police agent would be jeopardized if a backup team were not able to monitor the transaction and put a stop to it before any sexual act was culminated.

Accordingly, the defendant's motion to controvert the warrant and suppress the videotape is in all respects denied.



90 Misc.2d 673

Joan SHEEHAN, Plaintiff,

v.

Michael SHEEHAN, Defendant.

Supreme Court, Special Term,
Nassau County, Part V.

June 3, 1977.

Divorced wife, who obtained money judgment based on ex-husband's default in payment of alimony and child support, moved by order to show cause to compel bank, as trustee of funds deposited in profit sharing retirement plan, "Keogh Plan," to pay over to sheriff a sum sufficient to satisfy the judgment with interest. The Supreme Court, Eli Wager, J., held that the funds were in a "self-settled trust," that is, funds voluntarily paid over by depositor for his own ultimate benefit, revocable at will, and were not insulated from wife as ex-husband's creditor.

Plaintiff's motion granted.

an, further visual surveillance within the 30 day period became academic.

F.C.C. 71R-220

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION

WASHINGTON, D.C. 20554

<p>In Re Applications of ROBERTS FLYING SERVICE, INC., LAKELAND, FLA.</p> <p>LAKELAND FLYING SERVICE, INC., LAKELAND, FLA.</p> <p>For Aeronautical Advisory Station to Serve the Lakeland Municipal Airport, Lakeland, Fla.</p>	}	<p>Docket No. 18870 File No. 86-A-RL- 109</p> <p>Docket No. 18871 File No. 65-A-L-99</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	------------------------------------------------------------------------------------------------------

MEMORANDUM OPINION AND ORDER

(Adopted July 14, 1971; Released July 15, 1971)

BY THE REVIEW BOARD:

1. This proceeding involves the mutually exclusive applications of Roberts Flying Service, Inc. (Roberts) for renewal of its license for aeronautical advisory Station KJA7 serving Lakeland Municipal Airport, Lakeland, Florida, and of Lakeland Flying Service, Inc. (Lakeland) for authorization to construct such a station at the same location. The applications were designated for hearing by Commission Order, FCC 70-573, released June 9, 1970, 23 FCC 2d 592, on various issues, including *inter alia*, an issue to determine whether Roberts has operated its station in violation of the requirements of impartiality in supplying information as to the availability of ground services as set out by Section 87.257 of the Commission's Rules.¹ At the hearing, the Examiner initially sustained an objection by Roberts to the admissibility under Section 605 of the Communications Act of evidence Lakeland attempted to introduce to fulfill its burden of proceeding under this issue and consisting of communications between Roberts and aircraft in the vicinity. However, at the close of oral argument on March 8, 1971, the Examiner ruled that Section 605 was not applicable and that the record would be reopened to receive the evidence proffered by Lakeland. This ruling was formalized by Order, FCC 71M-364, released March 9, 1971. Roberts was given permission to appeal this ruling by the Examiner in an Order, FCC 71M-400, released March 15, 1971.

2. Presently before the Review Board is an appeal from the Examiner's Order reopening the record, filed May 6, 1971, by Roberts.² Roberts asserts that the Examiner's ruling appears to be based on three propositions: that communications over an aeronautical advisory (Unicom) station primarily involve safety, and, therefore, as a policy

¹ Both Roberts and Lakeland are suppliers of aircraft fuel.

² Related pleadings before the Review Board are: (a) opposition, filed May 12, 1971, by the Safety and Special Radio Services Bureau; and (b) reply, filed May 24, 1971, by Roberts.

matter, Section 605 should not apply; that Section 605 is not applicable because users of Unicom stations have no expectation of privacy; and that the use by Roberts of a loudspeaker system in its hangar area brings the communications here involved within the exception of Section 605 for radio communications broadcasts. In rebuttal, appellant first argues that most aeronautical advisory station communications do not relate to safety, and that, even if safety is involved, the safety exemption in Section 605 is limited solely to ships in distress, even though air-ground radio communications existed when the Section was enacted in 1934 and were fully developed in 1968 when it was amended by Congress. Further, Roberts denies that an expectation of privacy is relevant under Section 605, which, appellant contends, guards against interception *plus* unauthorized disclosure, since lack of expectation of privacy is inherent in radio transmissions. Appellant argues that if the Examiner's ruling is upheld "the protection accorded by Section 605 to radio communications, which by their very nature may be heard by anyone with a properly tuned receiver will be completely eroded." Finally, Roberts maintains that the Examiner could not properly base his ruling on the broadcast of the transmissions through a loudspeaker in Roberts' hangar. The loudspeaker did not convert them into transmissions which were broadcast generally because the hangar was not public property and Lakeland's witnesses did not gain the material for their testimony through that means.

3. In opposition, the Safety and Special Radio Services Bureau maintains that Section 605 does not apply because the frequencies used were allocated for aeronautical use and involved no element of privacy, citing *Brown v. CAB*, 324 F.2d 523 (1963). The Bureau argues that the interests of safety dictate the same result, since the Unicom system "is primarily a safety system for the benefit of all aircraft owners," and to apply Section 605 here would result in stopping a person from using an intercepted communication for his own safety. The Bureau also argues that Roberts' assumption that non-safety information is primarily involved in this case is not clear in the present posture of the case; that, even if it is assumed, *arguendo*, that Section 605 applies, the communications come within the exception which states that the section "shall not apply to receiving, divulging, publishing, or utilizing the contents of any radio communication which is . . . transmitted by . . . others for the use of the general public . . .", the general public here meaning the special class of all aviation users; and that to bar the testimony of non-Commission persons in enforcement and renewal proceedings would greatly reduce the Commission's ability to carry out its statutory mandate.

4. Roberts' appeal will be granted. None of the arguments made or cases cited by the Safety and Special Radio Services Bureau persuade us that Section 605 of the Communications Act is inapplicable to the instant situation. The type of unauthorized interception of radio communications involved here clearly comes within the language of that Section and, therefore, the evidence derived from such interception is inadmissible under the exclusionary rule established by judicial construction. *Nardone v. United States*, 302 U.S. 379 (1937). It is

equally clear that none of the specific statutory exceptions are applicable here, *i.e.*, the communications were not broadcast "for the use of the general public" and did not relate "to ships in distress." Nor does the possibility that some of the testimony of Lakeland's witnesses is based on safety communications render the proffered evidence admissible. What is involved here is not the hypothetical question of whether a crime would be committed by a pilot who intercepted and used information for the purposes of safety, but whether wrongly intercepted communications are admissible in evidence to aid the interceptor in making its case.³ The Bureau's argument that Section 605 cannot apply here because there could be no expectation of privacy by a user of an aeronautical advisory station must also be rejected. Section 605 prohibits unauthorized interception *plus* disclosure; it protects, not an expectation of full privacy, but an expectation that the user's message will not become generally public or be used to his detriment. See *U.S. v. Sugden*, 226 F.2d 281 (1955), affirmed, 351 U.S. 916 (1955).

5. While it has been judicially established that Commission personnel may intercept radio communications in furtherance of the Commission's enforcement responsibilities, there is no support for the Bureau's position that the Commission can rely upon outside interceptors of radio communications in enforcement and license renewal situations. *Brown v. CAB*, *supra*, which involved the recording by a control tower and subsequent use for purposes of license revocation of pilot-to-pilot conversations is distinguishable. That case does not establish an exception to Section 605 since the tower was a party to the communications from their inception when the petitioner initially called it for aid and was put in contact with the other pilot. Moreover, the Court stressed that the authorized aeronautical frequencies were assigned for the very purpose of permitting communications between traffic control personnel and pilots; that it was "standard procedure" to record communications with pilots; and that the conversations were permissible as evidence in the type of proceeding involved in *Brown*. That the instant situation does not come within any of the exceptions to Section 605 is supported by *U.S. v. Sugden*, *supra*, in which the Court held that even the Commission could not pass on intercepted communications to another government agency. The Court stated that the rules excluding evidence obtained in violation of Section 605 "are to be applied to listening in . . . on non-public broadcasts by both private individuals and all public officers save in connection with the Federal Communications Commission's necessary policing for violation of the act." Certainly, if the Commission's powers of interception and divulgence are so strictly limited, the power to divulge radio communications cannot be held to reside in non-Commission personnel, given the plain prohibitions of Section 605 and absent judicial construction or some indication of Congressional intent to the contrary. Therefore, for the above reasons, the Examiner's ruling will be set aside.

³ In fact, Roberts is correct in arguing in its reply pleading that such a use of intercepted communications would not be a crime within Section 605 for the lack of the requisite *mens rea*.

826

Federal Communications Commission Reports

6. Accordingly, **IT IS ORDERED**, That the Appeal from Hearing Examiner's Order Reopening the Record, filed May 6, 1971, by Roberts Flying Service, Inc., **IS GRANTED**, that the ruling contained in the Memorandum of Order Reopening Record, FCC 71M-364, released March 9, 1971, **IS REVERSED**, and that said Memorandum of Order **IS SET ASIDE**.

FEDERAL COMMUNICATIONS COMMISSION,
BEN F. WAPLE, *Secretary*.

30 F.C.C. 2d

101 Idaho 265

STATE of Idaho, Plaintiff-Respondent,

v.

Donald L. JENNINGS,
Defendant-Appellant.

No. 12919.

Supreme Court of Idaho.

May 30, 1980.

Defendant was convicted in the District Court, Third Judicial District, Canyon County, Robert B. Dunlap, J., of two counts of delivering heroin, and he appealed. The Supreme Court, Bistline, J., held that the evidence consisting of videotape and sound recordings made by police of the two transactions did not violate defendant's constitutionally protectable expectation of privacy nor his right against self-incrimination, and was admissible.

Affirmed.

1. Searches and Seizures ⇐7(1)

Fourth Amendment protects those claiming a justifiable, reasonable, or legitimate expectation of privacy from government-initiated electronic surveillance. U.S.C.A.Const. Amend. 4.

2. Searches and Seizures ⇐7(10)

Legitimate expectation of privacy means more than a subjective expectation of not being discovered. U.S.C.A.Const. Amend. 4.

3. Searches and Seizures ⇐7(1)

Fourth Amendment does not protect a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it; nor does it protect defendant where police informant records conversation on electronic equipment he carries on his person, or where informant carries electronic equipment which simultaneously transmits conversations either to recording equipment located elsewhere or to other agents monitoring transmitting frequency. U.S.C.A.Const. Amend. 4.

4. Criminal Law ⇐393(1), 394.1(2)

In prosecution for two counts of delivering heroin, evidence consisting of videotapes and sound recordings made by police of the two transactions, which took place in motel room rented and controlled by police in which concealed microphone and two-way mirror were installed, did not violate defendant's constitutionally protectable expectation of privacy nor his right against self-incrimination, and was admissible. U.S.C.A.Const. Amends. 4, 5.

Mark L. Clark of Kibler, Hamilton & Clark, Nampa, for defendant-appellant.

David H. Leroy, Atty. Gen., L. Mark Riddoch, Deputy Atty. Gen., Boise, for plaintiff-respondent.

BISTLINE, Justice.

Defendant-appellant Donald Jennings was convicted by a jury of two counts of delivering heroin. Before trial, the defendant moved to suppress videotapes and sound recordings made by the police of the two transactions. Defendant appeals from the judgment of conviction, challenging the order denying his motion to suppress.

For approximately six months (February to July 1977), the City-County Narcotics Division of Canyon County operated a "storefront" undercover operation at the Darling Motel in Caldwell. The Narcotics Division rented two adjacent rooms at the motel. One room (room no. 8) was set up as a normal motel room, but with a concealed microphone in the door jamb and a two-way mirror in the wall by which officers in the adjacent room could observe, videotape and record the transactions in room no. 8.

Mickey Parks, an undercover agent, used room no. 8 to conduct illegal activities, although he did not live there personally. The defendant and Parks both testified that the defendant had lived in room no. 8, but they disagreed as to when: defendant testified that as far as he knew he had lived there in March when the alleged transactions occurred, but he wasn't sure; Parks testified that the defendant lived there in

STATE v. JENNINGS

Idaho 1051

Cite as, Idaho, 611 P.2d 1050

May or June, but not in March. Lt. Galland, one of the officers operating the videotape equipment, testified that to his knowledge defendant was not living in room no. 8 in March, although he felt that the defendant was living in another room in the motel.

Lt. Galland also testified that he had observed the defendant through the two-way mirror between fifteen and twenty times. No search warrant was ever obtained, although Officer Galland testified that he would have gotten a warrant if the prosecuting attorney had advised him that he needed one.

On March 4 and 16, 1977, the officers in the adjoining room observed, videotaped and recorded the defendant allegedly delivering heroin to Parks. The officers testified to observing the transactions, and the tapes were shown to the jury.

Defendant argues on appeal that admitting the videotapes and recordings into evidence violated both his Fourth and Fifth Amendment rights, and that they should have been suppressed. He does not argue on appeal that the testimony of Parks or the officers as to their observations of the transactions should also have been excluded.

[1] The Fourth Amendment protects those claiming a "justifiable," a "reasonable," or a "legitimate" expectation of privacy from government-initiated electronic surveillance. *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 2580, 61 L.Ed.2d 220 (1979). See *United States v. White*, 401 U.S. 745, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971); *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

[2, 3] A legitimate expectation of privacy "means more than a subjective expectation of not being discovered." *Rakas v. Illinois*, 439 U.S. 128, 99 S.Ct. 421, 430 n.12, 58 L.Ed.2d 387 (1978). Thus the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Hoffa v. United States*, 385 U.S. 293, 302, 87 S.Ct. 408, 413,

17 L.Ed.2d 374 (1966). Nor does it protect the defendant where a police informant records the conversation on electronic equipment he carries on his person, *Lopez v. United States*, 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963), or where the informant carries electronic equipment "which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency." *United States v. White*, 401 U.S. 745, 751, 91 S.Ct. 1122, 1126, 28 L.Ed.2d 453 (1971). See also *United States v. Caceres*, 440 U.S. 741, 99 S.Ct. 1465, 59 L.Ed.2d 733 (1979). As stated in *Lopez v. United States*, 373 U.S. 427, 439, 83 S.Ct. 1381, 1388, 10 L.Ed.2d 462 (1963)

"[t]he Government did not use an electronic device to listen in on conversations it could not otherwise have heard. Instead, the device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose.

"Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory."

In *United States v. White*, 401 U.S. 745, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971), the court was confronted with the issue of "whether the Fourth Amendment bars from evidence the testimony of governmental agents who related certain conversations which had occurred between defendant White and a government informant, Harvey Jackson, and which the agents overheard by monitoring the frequency of a radio transmitter carried by Jackson and concealed on his person." *Id.* at 746-47, 91 S.Ct. at 1123 (footnote omitted). Four of the conversations took place in Jackson's

home, two took place in his car, one in a restaurant and one in defendant's home. The Court in a plurality opinion upheld the admissibility of the testimony as follows:

"Concededly a police agent who conceals his police connections may write down for official use his conversations with a defendant and testify concerning them, without a warrant authorizing his encounters with the defendant and without otherwise violating the latter's Fourth Amendment rights. *Hoffa v. United States*, 385 U.S. 293, at 300-303, [87 S.Ct. 408, at 412-414] 408, 17 L.Ed.2d 374. For constitutional purposes, no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person, *Lopez v. United States*, *supra*; (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency. *On Lee v. United States*, *supra* [343 U.S. 747, 72 S.Ct. 967, 96 L.Ed. 1270]. If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.

"Our problem is not what the privacy expectations of particular defendants in particular situations may be or the extent to which they may in fact have relied on the discretion of their companions. Very probably, individual defendants neither know nor suspect that their colleagues have gone or will go to the police or are carrying recorders or transmitters. Otherwise, conversation would cease and our problem with these encounters would be nonexistent or far different from those now before us. Our problem, in terms of the principles announced in *Katz*, is what

expectations of privacy are constitutionally 'justifiable'—what expectations the Fourth Amendment will protect in the absence of a warrant. So far, the law permits the frustration of actual expectations of privacy by permitting authorities to use the testimony of those associates who for one reason or another have determined to turn to the police, as well as by authorizing the use of informants in the manner exemplified by *Hoffa* and *Lewis* [*Lewis v. United States*, 385 U.S. 206, 87 S.Ct. 424, 17 L.Ed.2d 312]. If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case. See *Lopez v. United States*, 373 U.S. 427, [83 S.Ct. 1381, 10 L.Ed.2d 462] (1963).

"Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his. In terms of what his course will be, what he will or will not do or say, we are unpersuaded that he would distinguish between probable informers on the one hand and probable informers with transmitters on the other. Given the possibility or probability that one of his colleagues is cooperating with the police, it is only speculation to assert that the defendant's utterances would be substantially different or his sense of security any less if he also thought it possible that the suspected colleague is wired for sound. At least there is no persuasive evidence that the difference in this respect between the electronically equipped and the unequipped agent is substantial enough to require discrete constitutional recognition, particularly under the Fourth Amendment which is ruled by fluid concepts of 'reasonableness.'

STATE v. JENNINGS

Idaho 1053

Cite as, Idaho, 611 P.2d 1050

"Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent." 401 U.S. at 751-53, 91 S.Ct. at 1125-1126.

[4] Although the United States Supreme Court has not specifically dealt with the question before us, we find the reasoning in *White* controlling. The only other case dealing with a similar videotaping issue which we find,¹ *Avery v. State*, 15 Md. App. 520, 292 A.2d 728 (1972), cert. denied 410 U.S. 977, 93 S.Ct. 1499, 36 L.Ed.2d 173 (1973), also held *White* controlling. In that case, Miss Hall reported to the police that the defendant, a doctor, had sexually molested her. With the agreement of Miss Hall and her neighbor, the police installed a close-circuit television camera in Miss Hall's apartment and a monitor in the adjoining apartment. When defendant again visited Miss Hall in her apartment, he injected her intravenously, causing her to lose consciousness, and he then began sexually molesting her. This time, however the whole incident was taped and observed by those watching the monitor. The court held that the tape was admissible:

"[I]n the instant case we have an electronic interception and video transmission of the conduct of the accused toward the victim while in the victim's house which was transmitted to the police with the full cooperation and consent of the victim as a party to that conduct. The situation here is comparable to one where the conversations between a government agent and the accused are transmitted to police authority by a radio transmitter secreted on the person of the government agent (informer) with the cooperation and ap-

proval of the agent. If the transmittal of the verbal conversation to the police through the cooperation of an informer does not constitute an unreasonable seizure in violation of a 'justifiable expectation of privacy' in *White*, we see no good or sufficient reason to conclude that a video transmittal of the accused's conduct brought about by the cooperation of Miss Hall should be interpreted as constituting an unreasonable seizure in violation of the appellant's 'justifiable expectation of privacy' in the instant case." 292 A.2d at 742-43.

Defendant attempts to distinguish *White* on two grounds: (1) *White* dealt with electronic monitoring of a conversation rather than videotaping, and (2) unlike in *White*, none of the electronic devices used here were on the person of the government agent. As to the first distinction, we can see no reason why a person's justifiable expectations of privacy would be greater where videotapes are made than where just sound recordings are made. It is not the nature of the recording that is at issue but whether the defendant has an expectation of privacy such that any recording would violate the Fourth Amendment. The defendant is relying on the discretion of the person to whom he is talking, and just as that person can testify as to statements made by the defendant, *Lopez v. United States*, 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963), so he can testify as to physical actions of the defendant. The videotapes, just like the sound recordings, simply produce the most reliable evidence of the actual transaction, and there is no apparent reason why a sound recording should be admissible and a videotape inadmissible.

The second distinction drawn by the defendant, although much more troublesome,

1. Defendant cites *People v. Teicher*, 90 Misc.2d 638, 395 N.Y.S.2d 587 (Sup. 1977), in support of his contention that a warrant is required. In that case the state obtained a warrant and installed videotape equipment in a dentist's office, and subsequently taped the defendant-dentist sexually molesting a patient. The court held that the videotape was admissible, and the

defendant urges that this illustrates the necessity of obtaining a search warrant before installing video equipment. That case is distinguishable, however, because the court never discussed whether a warrant was required and because it involved entering the defendant's office in order to install the taping equipment.

is also not controlling. Although we are aware of the dangerous potential of an Orwellian state inherent in universal uncontrolled electronic monitoring and videotaping by the State, see, e. g., Fried, *Privacy*, 77 Yale L.J. 475 (1968); H. Schwartz, *Taps, Bugs and Fooling the People* (1977); *Electronic Visual Surveillance and the Fourth Amendment: The Arrival of Big Brother?*, 3 Hastings Const.L.Q. 261 (1976), we do not feel that the use of recordings by the police in their "storefront operations" where they control the rooms and where their agent is involved in the transaction poses such a threat. This is not a case of electronic snooping, where the police indiscriminately monitor motel rooms to discover what is happening in them. See, e. g., 3 Hastings Const.L.Q., *supra*. Nor is this a case where the police had to surreptitiously enter the abode of another in order to install the recording equipment. See, e. g., *United States v. Ford*, 553 F.2d 146 (D.C. Cir. 1977); *Judicial Acceptance of Video Tape as Evidence*, 16 Am.Crim.L.Rev. 183, 192-93 (1978).

This is simply a case where the defendant entered a room controlled by the police and sold heroin to a police agent in that room.² The defendant's expectation of privacy was that Parks would not tell the police of the transaction; just as that expectation is not constitutionally protectable, so there is no constitutional prohibition against admission of the tape where Parks consented to the filming.

Defendant also argues that his Fifth Amendment rights against self-incrimination were violated. Defendant cites no authority to support his position; instead he simply argues that allowing the jury to watch and listen to the defendant on film for approximately one hour where defendant had not freely consented to the filming violated his Fifth Amendment rights.

2. Defendant argues that his expectation of privacy is greater here because he was living in the room no. 8 and paying rent to Mickey Parks. However, his testimony was very indefinite as to whether or when he was living in room no. 8, while Parks testified that defendant was not living there at the times that the recordings were made, and Lt. Galland testified

In *United States v. Craig*, 573 F.2d 455 (7th Cir. 1977), cert. denied 439 U.S. 820, 99 S.Ct. 82, 58 L.Ed.2d 110 (1978), the court held admissible a recording made of a phone conversation where one party had consented to the recording. With regard to defendant's argument that his Fifth Amendment rights had been violated, the court held as follows:

"Further, Walker's contention that his Fifth Amendment rights were violated since he should have been made aware of his rights prior to making any statement is of no avail. Advice of rights is required in custodial situations where the inherent pressures to speak in the face of governmental authority are present. *Beckwith v. United States*, 425 U.S. 341, 96 S.Ct. 1612, 48 L.Ed.2d 1; *United States v. Gardner*, 516 F.2d 334 (7th Cir. 1975), cert. denied, 423 U.S. 861, 96 S.Ct. 118, 46 L.Ed.2d 89 (1975). As Judge Bauer stated in *United States v. Bastone*, *supra*, 526 F.2d at 977:

'A person is not entitled to warnings simply because an investigation has focused upon him. The test is not focus alone, but rather, focus plus custodial interrogation. *Escobedo v. Illinois*, 378 U.S. 478, 84 S.Ct. 1758, 12 L.Ed.2d 977 (1964); *Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966).'

"While it is clear the investigation had focused upon defendant Walker, his recorded conversations with Carpentier involved no confrontation with governmental authority in the context of a custodial interrogation calling for *Miranda* warnings. Consequently, we must reject Walker's contention that the recordings violated his Fifth Amendment rights." 573 F.2d at 474.

that to his knowledge defendant was not living there at the time the tapes were made, but was living in another room in the motel. Since the police originally rented the room and apparently had control over it, this argument fails to persuade us that the trial court erred in denying the motion to suppress.

WINN v. WINN

Idaho 1055

Cite as, Idaho, 611 P.2d 1055

In *People v. Feneion*, 14 Ill.App.3d 622, 303 N.E.2d 38 (1973), the court held that the waiver of *Miranda* rights is not a prerequisite to the admission of a video recording of physical tests to determine intoxication. The court reasoned that where the evidence of the tests themselves is admissible, then the recording of those tests is admissible.

The United States Supreme Court in *Hoffa v. United States*, 385 U.S. 293, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966), although not concerned with electronic surveillance, held that "a necessary element of compulsory self-incrimination is some kind of compulsion." *Id.* at 304, 87 S.Ct. at 414. As noted in that case, "[i]n the present case no claim has been or could be made that the petitioner's incriminating statements were the product of any sort of coercion, legal or factual." *Id.* Defendant here acted voluntarily, and the recordings of his acts, just like the eyewitness testimony to his acts, are admissible.

Affirmed.

DONALDSON, C. J., and SHEPARD, BAKES and McFADDEN, JJ., concur.



101 Idaho 270
Virgil George WINN,
Plaintiff-Respondent,

v.

Alfreda E. WINN, Defendant-Appellant.

No. 12951.

Supreme Court of Idaho.

June 2, 1980.

Wife appealed from an order of the District Court, Fourth Judicial District, Ada County, Jesse R. Walters, J., which reversed magistrate's decision in a divorce action and ordered a trial de novo in the district court. The Supreme Court, Bakes, J., held that:

(1) district judge was justified in ordering trial de novo of divorce action wherein house in which parties resided was determined to be community property, where magistrate's memorandum opinion was conclusory and failed to set forth rationale underlying his decision, notwithstanding fact that district court also conducted appellate review and eventually concluded that magistrate's disposition was not supported by substantial evidence and was not in conformity with applicable law, and (2) order for trial de novo precluded appeal of district court's decision.

Appeal dismissed.

McFadden, J., filed specially concurring opinion.

Bistline, J., filed dissenting opinion.

1. Justices of the Peace ⇔ 147(1)

Decisions by district court dismissing, affirming, or reversing or remanding appeal are appealable. Appellate Rules, Rule 11(a)(1).

2. Justices of the Peace ⇔ 171(1)

District court may conduct appellate review of magistrate's decision or district court may choose to wipe slate clean by ordering trial de novo and beginning case anew. Rules of Civil Procedure, Rule 83(b, u); I.C. § 1-2213(2).

3. Justices of the Peace ⇔ 171(1)

District court, having undertaken task of conducting appellate review of magistrate's decision, is not as a result precluded from conducting trial de novo. Rules of Civil Procedure, Rule 83(b, u).

4. Justices of the Peace ⇔ 164(4)

When circumstances prevent decisive, complete, or meaningful appellate review of magistrate's decision, it may be advisable for district court to augment trial record or create new record in order completely to resolve the controversy; this occurs where trial court's findings of fact are confused or in conflict, or where findings on particular issue are lacking, and resort to record does not show clearly what findings are correct. Rules of Civil Procedure, Rule 83(b, u).

RICHMOND UNIFIED SCHOOL DISTRICT *v.* BERG

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR
THE NINTH CIRCUIT

No. 75-1069. Argued October 5, 1977—Decided December 6, 1977

528 F. 2d 1208, vacated and remanded.

Arthur W. Walenta, Jr., argued the cause for petitioners. With him on the briefs was *John B. Clausen*.

Mary C. Dunlap argued the cause and filed a brief for respondent.*

PER CURIAM.

The judgment of the Court of Appeals, 528 F. 2d 1208, is vacated and the cause remanded for further consideration in light of *General Electric Co. v. Gilbert*, 429 U. S. 125 (1976), and *Nashville Gas Co. v. Satty*, *ante*, p. 136, and for consideration of possible mootness.

**Jerry D. Anker, Robert E. Nagle, and David Rubin* filed a brief for the National Education Assn. as *amicus curiae* urging affirmance.

Syllabus

UNITED STATES *v.* NEW YORK TELEPHONE CO.CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE
SECOND CIRCUIT

No. 76-835. Argued October 3, 1977—Decided December 7, 1977

On the basis of an FBI affidavit stating that certain individuals were conducting an illegal gambling enterprise at a specified New York City address and that there was probable cause to believe that two telephones with different numbers were being used there to further the illegal activity, the District Court authorized the FBI to install and use pen registers with respect to the two telephones, and directed respondent telephone company to furnish the FBI "all information, facilities and technical assistance" necessary to employ the devices, which (without overhearing oral communications or indicating whether calls are completed) record the numbers dialed. The FBI was ordered to compensate respondent at prevailing rates. Respondent, though providing certain information, refused to lease to the FBI lines that were needed for unobtrusive installation of the pen registers, and thereafter filed a motion in the District Court to vacate that portion of the pen register order directing respondent to furnish facilities and technical assistance to the FBI, on the ground that such a directive could be issued only in connection with a wiretap order meeting the requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The District Court ruled adversely to respondent, holding that pen registers are not governed by Title III; that the court had jurisdiction to authorize installation of the devices upon a showing of probable cause; and that it had authority to direct respondent to assist in the installation both under the court's inherent powers and under the All Writs Act, which gives federal courts authority to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." Though agreeing with the District Court's Title III rationale, and concluding that district courts have power either inherently or as a logical derivative of Fed. Rule Crim. Proc. 41, to authorize pen register surveillance upon a probable-cause showing, the Court of Appeals, affirming in part and reversing in part, held that the District Court abused its discretion in ordering respondent to assist in installing and operating the pen registers, and expressed concern that such a requirement could establish an undesirable precedent for the authority of federal courts to impress unwilling aid on private third parties. *Held:*

1. Title III, which is concerned only with orders "authorizing or approving the *interception* of a wire or oral communication," does not govern the authorization of the use of pen registers, which do not "intercept" because they do not acquire the "contents" of communications as those terms are defined in the statute. Moreover, the legislative history of Title III shows that the definition of "intercept" was designed to exclude pen registers. Pp. 165-168.

2. The District Court under Fed. Rule Crim. Proc. 41 had power to authorize the installation of the pen registers, that Rule being sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause. Pp. 168-170.

3. The order compelling respondent to provide assistance was clearly authorized by the All Writs Act and comported with the intent of Congress. Pp. 171-178.

(a) The power conferred by the Act extends, under appropriate circumstances, to persons who (though not parties to the original action or engaged in wrongdoing) are in a position to frustrate the implementation of a court order or the proper administration of justice. Here respondent, which is a highly regulated public utility with a duty to serve the public, was not so far removed as a third party from the underlying controversy that its assistance could not permissibly be compelled by the order of the court based on a probable-cause showing that respondent's facilities were being illegally used on a continuing basis. Moreover, respondent concededly uses the devices for its billing operations, detecting fraud, and preventing law violations. And, as the Court of Appeals recognized, provision of a leased line by respondent was essential to fulfillment of the purpose for which the pen register order had been issued. Pp. 171-175.

(b) The District Court's order was consistent with a 1970 amendment to Title III providing that "[a]n order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier . . . furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively. . . ." Pp. 176-177.

538 F. 2d 956, reversed.

WHITE, J., delivered the opinion of the Court, in which BURGER, C. J., and BLACKMUN, POWELL, and REHNQUIST, JJ., joined; in Parts I, II, and III of which STEWART, J., joined; and in Part II of which BRENNAN, MARSHALL, and STEVENS, JJ., joined. STEWART, J., filed an opinion concurring in part and dissenting in part, *post*, p. 178. STEVENS, J., filed an

UNITED STATES *v.* NEW YORK TELEPHONE CO. 1

159

Opinion of the Court

opinion dissenting in part, in which BRENNAN and MARSHALL, JJ., joined and in Part II of which STEWART, J., joined, *post*, p. 178.

Deputy Solicitor General Wallace argued the cause for the United States and was on the brief as Acting Solicitor General. With him on the brief were *Assistant Attorney General Civiletti*, *Deputy Solicitor General Randolph*, *Harriet Shapiro*, *Jerome M. Feit*, and *Marc Philip Richman*.

George E. Ashley argued the cause for respondent. With him on the brief was *Frank R. Natoli*.

MR. JUSTICE WHITE delivered the opinion of the Court.

This case presents the question of whether a United States District Court may properly direct a telephone company to provide federal law enforcement officials the facilities and technical assistance necessary for the implementation of an order authorizing the use of pen registers¹ to investigate offenses which there was probable cause to believe were being committed by means of the telephone.

I

On March 19, 1976, the United States District Court for the Southern District of New York issued an order authorizing agents of the Federal Bureau of Investigation (FBI) to install and use pen registers with respect to two telephone numbers and directing the New York Telephone Co. (Company) to furnish the FBI "all information, facilities and technical assistance" necessary to employ the pen registers unobtrusively. The FBI was ordered to compensate the Company at prevailing rates for any assistance which it furnished. App. 6-7. The order was issued on the basis of an affidavit sub-

¹ A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.

mitted by an FBI agent which stated that certain individuals were conducting an illegal gambling enterprise at 220 East 14th Street in New York City and that, on the basis of facts set forth therein, there was probable cause to believe that two telephones bearing different numbers were being used at that address in furtherance of the illegal activity. *Id.*, at 1-5. The District Court found that there was probable cause to conclude that an illegal gambling enterprise using the facilities of interstate commerce was being conducted at the East 14th Street address in violation of 18 U. S. C. §§ 371 and 1952, and that the two telephones had been, were currently being, and would continue to be used in connection with those offenses. Its order authorized the FBI to operate the pen registers with respect to the two telephones until knowledge of the numbers dialed led to the identity of the associates and confederates of those believed to be conducting the illegal operation or for 20 days, "whichever is earlier."

The Company declined to comply fully with the court order. It did inform the FBI of the location of the relevant "appearances," that is, the places where specific telephone lines emerge from the sealed telephone cable. In addition, the Company agreed to identify the relevant "pairs," or the specific pairs of wires that constituted the circuits of the two telephone lines. This information is required to install a pen register. The Company, however, refused to lease lines to the FBI which were needed to install the pen registers in an unobtrusive fashion. Such lines were required by the FBI in order to install the pen registers in inconspicuous locations away from the building containing the telephones. A "leased line" is an unused telephone line which makes an "appearance" in the same terminal box as the telephone line in connection with which it is desired to install a pen register. If the leased line is connected to the subject telephone line, the pen register can then be installed on the leased line at a remote location and be monitored from that point. The

UNITED STATES v. NEW YORK TELEPHONE CO.

159

Opinion of the Court

Company, instead of providing the leased lines, which conceded that the court's order required it to do, advised the FBI to string cables from the "subject apartment" to another location where pen registers could be installed. The FBI determined after canvassing the neighborhood of the apartment for four days that there was no location where it could string its own wires and attach the pen registers without alerting the suspects,² in which event, of course, the gambling operation would cease to function. App. 15-22.

On March 30, 1976, the Company moved in the District Court to vacate that portion of the pen register order directing it to furnish facilities and technical assistance to the FBI in connection with the use of the pen registers on the ground that such a directive could be issued only in connection with a wiretap order conforming to the requirements of Title I of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U. S. C. §§ 2510-2520 (1970 ed. and Supp. V). It contended that neither Fed. Rule Crim. Proc. 41 nor the All Writs Act, 28 U. S. C. § 1651 (a), provided any basis for such an order. App. 10-14. The District Court ruled that pen registers are not governed by the proscriptions of Title I because they are not devices used to intercept oral communications. It concluded that it had jurisdiction to authorize the installation of the pen registers upon a showing of probable cause and that both the All Writs Act and its inherent powers provided authority for the order directing the Company to assist in the installation of the pen registers.

On April 9, 1976, after the District Court and the Court of Appeals denied the Company's motion to stay the pen register order pending appeal, the Company provided the leased lines.³

² The gambling operation was known to employ countersurveillance techniques. App. 21.

³ On the same date another United States District Court judge extended the original order of March 19 for an additional 20 days. *Id.*, at 33.

OCTOBER TERM, 1977

Opinion of the Court

434 U.S.

The Court of Appeals affirmed in part and reversed in part, with one judge dissenting on the ground that the order below should have been affirmed in its entirety. *Application of United States in re Pen Register Order*, 538 F. 2d 956 (CA2 1976). It agreed with the District Court that pen registers do not fall within the scope of Title III and are not otherwise prohibited or regulated by statute. The Court of Appeals also concluded that district courts have the power, either inherently or as a logical derivative of Fed. Crim. Proc. 41, to authorize pen register surveillance upon an adequate showing of probable cause. The majority held, however, that the District Court abused its discretion in ordering the Company to assist in the installation and operation of the pen registers. It assumed, *arguendo*, that "a district court has inherent discretionary authority or discretionary power under the All Writs Act to compel technical assistance by the Telephone Company," but concluded that "in the absence of specific and properly limited Congressional action, it was an abuse of discretion for the District Court to order the Telephone Company to furnish technical assistance." 538 F. 2d, at 961.⁴ The majority expressed concern that "such an order could establish a most undesirable, if not dangerous and unwise, precedent for the authority of federal courts to impress unwilling aid on private third parties" and that "there is no assurance that the court will always be able to protect [third parties] from excessive or overzealous Government activity or compulsion." *Id.*, at 962-963.⁵

⁴ The Court of Appeals recognized that "without [the Company's] technical aid, the order authorizing the use of a pen register will be worthless. Federal law enforcement agents simply cannot implement pen register surveillance without the Telephone Company's help. The assistance requested requires no extraordinary expenditure of time or effort by [the Company]; indeed, as we understand it, providing lease or private lines is a relatively simple, routine procedure." 538 F. 2d, at 961-962.

⁵ Judge Mansfield dissented in part on the ground that the District Court possessed a discretionary power under the All Writs Act to direct the

UNITED STATES .v. NEW YORK TELEPHONE CO.

159

Opinion of the Court

We granted the United States' petition for certiorari challenging the Court of Appeals' invalidation of the District Court's order against respondent.⁶ 429 U. S. 1072.

II

We first reject respondent's contention, which is renewed here, that the District Court lacked authority to order the Company to provide assistance because the use of pen registers may be authorized only in conformity with the procedure set forth in Title III⁷ for securing judicial authority to int

Company to render such assistance as was necessary to implement its order authorizing the use of pen registers and that a compelling case has been established for the exercise of discretion in favor of the assistance order. He argued that district court judges could be trusted to exercise their powers under the All Writs Act only in cases of clear necessity to balance the burden imposed upon the party required to render assistance against the necessity.

⁶ Although the pen register surveillance had been completed by the time the Court of Appeals issued its decision on July 13, 1976, this fact does not render the case moot, because the controversy here is one "capable of repetition, yet evading review." *Southern Pacific Terminal Co. v. I* 219 U. S. 498, 515 (1911); *Roe v. Wade*, 410 U. S. 113, 125 (1973). Pen register orders issued pursuant to Fed. Rule Crim. Proc. 41 authorize surveillance only for brief periods. Here, despite expedited action by the Court of Appeals, the order, as extended, expired six days after argument. Moreover, even had the pen register order been stayed pending appeal, the mootness problem would have remained, because the showing of probable cause upon which the order authorizing the installation of pen registers was based would almost certainly have become stale before review could have been completed. It is also plain, given the Company's policy of refusing to render voluntary assistance in installing pen registers and the Government's determination to continue to utilize them, that the Company will be subjected to similar orders in the future. See *Weins v. Bradford*, 423 U. S. 147, 149 (1975).

⁷ The Court of Appeals held that pen register surveillance was subject to the requirements of the Fourth Amendment. This conclusion is not challenged by either party, and we find it unnecessary to consider the matter. The Government concedes that its application for the pen register order does not conform to the requirements of Title III.

cept wire communications.⁸ Both the language of the statute and its legislative history establish beyond any doubt that pen registers are not governed by Title III.⁹

Title III is concerned only with orders “authorizing or approving the *interception* of a wire or oral communication” 18 U. S. C. § 2518 (1) (emphasis added).¹⁰ Congress defined “intercept” to mean “the *aural* acquisition of the *contents* of any wire or oral *communication* through the use of any electronic, mechanical, or other device.” 18 U. S. C.

⁸ Although neither this issue nor that of the scope of Fed. Rule Crim. Proc. 41 is encompassed within the question posed in the petition for certiorari and the Company has not filed a cross-petition, we have discretion to consider them because the prevailing party may defend a judgment on any ground which the law and the record permit that would not expand the relief it has been granted. *Langnes v. Green*, 282 U. S. 531, 538-539 (1931); *Dandridge v. Williams*, 397 U. S. 471, 475 n. 6 (1970). The only relief sought by the Company is that granted by the Court of Appeals: the reversal of the District Court’s order directing it to assist in the installation and operation of the pen registers. The Title III and Rule 41 questions were considered by both the District Court and the Court of Appeals and fully argued here.

⁹ Four Justices reached this conclusion in *United States v. Giordano*, 416 U. S. 505, 553-554 (1974) (POWELL, J., joined by BURGER, C. J., and BLACKMUN and REHNQUIST, JJ., concurring in part and dissenting in part). The Court’s opinion did not reach the issue since the evidence derived from a pen register was suppressed as being in turn derived from an illegal wire interception. Every Court of Appeals that has considered the matter has agreed that pen registers are not within the scope of Title III. See *United States v. Illinois Bell Tel. Co.*, 531 F. 2d 809 (CA7 1976); *United States v. Southwestern Bell Tel. Co.*, 546 F. 2d 243 (CA8 1976); *Michigan Bell Tel. Co. v. United States*, 565 F. 2d 385 (CA6 1977); *United States v. Falcone*, 505 F. 2d 478 (CA3 1974), cert. denied, 420 U. S. 955 (1975); *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F. 2d 254 (CA9 1977); *United States v. Clegg*, 509 F. 2d 605, 610 n. 6 (CA5 1975).

¹⁰ Similarly, the sanctions of Title III are aimed only at one who “willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication” 18 U. S. C. § 2511 (1)(a).

§ 2510 (4) (emphasis added). Pen registers do not “intercept” because they do not acquire the “contents” of communications, as that term is defined by 18 U. S. C. § 2510 (8).¹¹ Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers. Furthermore, pen registers do not accomplish the “aural acquisition” of anything. They decode outgoing telephone numbers by responding to changes in electrical voltage caused by the turning of the telephone dial (or the pressing of buttons on pushbutton telephones) and present the information in a form to be interpreted by sight rather than by hearing.¹²

The legislative history confirms that there was no congressional intent to subject pen registers to the requirements of Title III. The Senate Report explained that the definition of “intercept” was designed to exclude pen registers:

“Paragraph 4 [of § 2510] defines ‘intercept’ to include the aural acquisition of the contents of any wire or oral communication by any electronic, mechanical, or other device. Other forms of surveillance are not within the proposed legislation. . . . The proposed legislation is not designed to prevent the tracing of phone calls. The use of a ‘pen register,’ for example, would be permissible. But see *United States v. Dote*, 371 F. 2d 176 (7th 1966). The proposed legislation is intended to protect the privacy of the communication itself and not the means of

¹¹ “‘Contents’ . . . includes any information concerning the identity of the parties to [the] communication or the existence, substance, purport, or meaning of [the] communication.”

¹² See 538 F. 2d, at 957.

communication." S. Rep. No. 1097, 90th Cong., 2d Sess., 90 (1968).¹³

It is clear that Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications and did not intend to impose Title III restrictions upon their use.

III

We also agree with the Court of Appeals that the District Court had power to authorize the installation of the pen registers.¹⁴ It is undisputed that the order in this case was predicated upon a proper finding of probable cause, and no claim is made that it was in any way inconsistent with the

¹³ *United States v. Dote*, 371 F. 2d 176 (CA7 1966), held that § 605 of the Communications Act of 1934, 47 U. S. C. § 605, which prohibited the interception and divulgence of "any communication" by wire or radio, included pen registers within the scope of its ban. In § 803 of Title III, 82 Stat. 223, Congress amended § 605 by restricting it to the interception of "any radio communication." Thus it is clear that pen registers are no longer within the scope of § 605. See *Korman v. United States*, 486 F. 2d 926, 931-932 (CA7 1973). The reference to *Dote* in the Senate Report is indicative of Congress' intention not to place restrictions upon their use. We find no merit in the Company's suggestion that the reference to *Dote* is merely an oblique expression of Congress' desire that telephone companies be permitted to use pen registers in the ordinary course of business, as *Dote* allowed, so long as they are not used to assist law enforcement. Brief for Respondent 16. The sentences preceding the reference to *Dote* state unequivocally that pen registers are not within the scope of Title III. In addition, a separate provision of Title III, 18 U. S. C. § 2511 (2) (a) (i), specifically excludes all normal telephone company business practices from the prohibitions of the Act. Congress clearly intended to disavow *Dote* to the extent that it prohibited the use of pen registers by law enforcement authorities.

¹⁴ The Courts of Appeals that have considered the question have agreed that pen register orders are authorized by Fed. Rule Crim. Proc. 41 or by an inherent power closely akin to it to issue search warrants under circumstances conforming to the Fourth Amendment. See *Michigan Bell Tel. Co.*, *supra*; *Southwestern Bell Tel. Co.*, *supra*; *Illinois Bell Tel. Co.*, *supra*.

Fourth Amendment. Federal Rule Crim. Proc. 41 (b) authorizes the issuance of a warrant to:

“search for and seize any (1) property that constitute evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense.”

This authorization is broad enough to encompass a “search” designed to ascertain the use which is being made of a telephone suspected of being employed as a means of facilitating a criminal venture and the “seizure” of evidence which the “search” of the telephone produces. Although Rule 41 (h) defines property “to include documents, books, papers and any other tangible objects,” it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41.¹⁵ Indeed, we recognized in *Katz v. United States*, 389 U. S. 347 (1967), which held that telephone conversations were protected by the Fourth Amendment, that Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause. 389 U. S., at 354–356 and n. 16.¹⁶ See also *Osborn v. United States*, 385 U. S. 323–329–331 (1966).

¹⁵ Where the definition of a term in Rule 41 (h) was intended to be inclusive, it is introduced by the phrase “to mean” rather than “to include.” Cf. *Helvering v. Morgan's, Inc.*, 293 U. S. 121, 125 n. 1 (1934).

¹⁶ The question of whether the FBI, in its implementation of the District Court's pen register authorization, complied with all the requirements of Rule 41 is not before us. In *Katz*, the Court stated that the notice requirement of Rule 41 (d) is not so inflexible as to require invariably that notice be given the person “searched” prior to the commencement of the search. 389 U. S., at 355–356, n. 16. Similarly, it is clear to us that the requirement of Rule 41 (c) that the warrant command that the search be conducted within 10 days of its issuance does not mean that the duration of a pen register surveillance may not exceed 10 days. Thu

Our conclusion that Rule 41 authorizes the use of pen registers under appropriate circumstances is supported by Fed. Rule Crim. Proc. 57 (b), which provides: "If no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or with any applicable statute."¹⁷ Although we need not and do not decide whether Rule 57 (b) by itself would authorize the issuance of pen register orders, it reinforces our conclusion that Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers as well as tangible items.

Finally, we could not hold that the District Court lacked any power to authorize the use of pen registers without defying the congressional judgment that the use of pen registers "be permissible." S. Rep. No. 1097, *supra*, at 90. Indeed, it would be anomalous to permit the recording of conversations by means of electronic surveillance while prohibiting the far lesser intrusion accomplished by pen registers. Congress intended no such result. We are unwilling to impose it in the absence of some showing that the issuance of such orders would be inconsistent with Rule 41. Cf. Rule 57 (b), *supra*.¹⁸

the District Court's order, which authorized surveillance for a 20-day period, did not conflict with Rule 41.

¹⁷ See *United States v. Baird*, 414 F. 2d 700, 710 (CA2 1969), cert. denied, 396 U. S. 1005 (1970); *Jackson v. United States*, 122 U. S. App. D. C. 324, 326, 353 F. 2d 862, 864 (1965); *United States v. Remolis*, 227 F. Supp. 420, 423 (Nev. 1964); *Link v. Wabash R. Co.*, 370 U. S. 626, 633 n. 8 (1962) (applying the analogous provision of Fed. Rule Civ. Proc. 83).

¹⁸ The dissent argues, *post*, at 182-184, that Rule 41 (b), as modified following *Warden v. Hayden*, 387 U. S. 294 (1967), to explicitly authorize searches for any property that constitutes evidence of a crime, falls short of authorizing warrants to "search" for and "seize" intangible evidence. The elimination of the restriction against seizing property that is "mere evidence," however, has no bearing whatsoever on the scope of the definition of property set forth in Rule 41 (b) which, as the dissent acknowledges, remained unchanged. Moreover, the definition of property set forth in

UNITED STATES *v.* NEW YORK TELEPHONE CO.

159

Opinion of the Court

IV

The Court of Appeals held that even though the District Court had ample authority to issue the pen register warrant and even assuming the applicability of the All Writs Act, the order compelling the Company to provide technical assistance constituted an abuse of discretion. Since the Court of Appeals conceded that a compelling case existed for requiring the assistance of the Company and did not point to any fact particular to this case which would warrant a finding of abuse of discretion, we interpret its holding as generally barring district courts from ordering any party to assist in the installation or operation of a pen register. It was apparently concerned that sustaining the District Court's order would authorize courts to compel third parties to render assistance without limitation regardless of the burden involved and pose a severe threat to the autonomy of third parties who, for whatever reason prefer not to render such assistance. Consequently the Court of Appeals concluded that courts should

Rule 41 (h) is introduced by the phrase, "[t]he term 'property' is used in this rule to *include*" (emphasis added), which indicates that it was intended to be exhaustive. See *supra*, at 169.

We are unable to comprehend the logic supporting the dissent's contention, *post*, at 184-185, that the conclusion of *Katz v. United States* that Rule 41 was not confined to tangible property did not survive the enactment of Title III and Title IX of the Omnibus Crime Control and Safe Streets Act of 1968, because Congress failed to expand the definition of property contained in Rule 41 (h). There was obviously no need for such an action in light of the Court's construction of the Rule in *Katz*. The dissent's assertion that it "strains credulity" to conclude that Congress intended to permit the seizure of intangibles outside the scope of Title III without its safeguards disregards the congressional judgment that the use of pen registers be permissible without Title III restrictions. Indeed, the dissent concedes that pen registers are not governed by Title III. What "strains credulity" is the dissent's conclusion, directly contradicted by the legislative history of Title III, that Congress intended to permit the interception of telephone conversations while prohibiting the use of pen registers to obtain much more limited information.

embark upon such a course without specific legislative authorization. We agree that the power of federal courts to impose duties upon third parties is not without limits; unreasonable burdens may not be imposed. We conclude, however, that the order issued here against respondent was clearly authorized by the All Writs Act and was consistent with the intent of Congress.¹⁹

The All Writs Act provides:

“The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.” 28 U. S. C. § 1651 (a).

The assistance of the Company was required here to implement a pen register order which we have held the District Court was empowered to issue by Rule 41. This Court has repeatedly recognized the power of a federal court to issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained: “This statute has served since its inclusion, in substance, in the original Judiciary Act as a ‘legislatively approved source of procedural instruments designed to achieve “the rational ends of law.”’” *Harris v. Nelson*, 394 U. S. 286, 299 (1969), quoting *Price v. Johnston*, 334 U. S. 266, 282 (1948). Indeed, “[u]nless appropriately confined by

¹⁹ The three other Courts of Appeals which have considered the question reached a different conclusion from the Second Circuit. The Sixth Circuit in *Michigan Bell Tel. Co. v. United States*, 565 F. 2d 385 (1977), and the Seventh Circuit in *United States v. Illinois Bell Tel. Co.*, 531 F. 2d 809 (1976), held that the Act did authorize the issuance of orders compelling a telephone company to assist in the use of surveillance devices not covered by Title III such as pen registers. The Eighth Circuit found such authority to be part of the inherent power of district courts and “concomitant of the power to authorize pen register surveillance.” *United States v. Southwestern Bell Tel. Co.*, 546 F. 2d, at 246.

UNITED STATES *v.* NEW YORK TELEPHONE CO.

159

Opinion of the Court

Congress, a federal court may avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it." *Adams v. United States ex rel. McCann*, 317 U. S. 269, 273 (1942).

The Court has consistently applied the Act flexibly in conformity with these principles. Although § 262 of the Judicial Code, the predecessor to § 1651, did not expressly authorize courts, as does § 1651, to issue writs "appropriate" to the proper exercise of their jurisdiction but only "necessary" writs, *Adams* held that these supplemental powers are not limited to those situations where it is "necessary" to issue the writ or order "in the sense that the court could not otherwise physically discharge its appellate duties." 317 U. S., at 273. In *Price v. Johnston, supra*, § 262 supplied the authority for the United States Court of Appeals to issue an order commanding that a prisoner be brought before the court for the purpose of arguing his own appeal. Similarly, in order to avoid frustrating the "very purpose" of 28 U. S. C. § 2255, § 1651 furnished the District Court with authority to order that a federal prisoner be produced in court for purposes of a hearing. *United States v. Hayman*, 342 U. S. 205, 220-222 (1952). The question in *Harris v. Nelson, supra*, was whether, despite the absence of specific statutory authority, the District Court could issue a discovery order in connection with a habeas corpus proceeding pending before it. Eight Justices agreed that the district courts have power to require discovery when essential to render a habeas corpus proceeding effective. The Court has also held that despite the absence of express statutory authority to do so, the Federal Trade Commission may petition for an order and a Court of Appeals may issue, pursuant to § 1651, an order preventing a merger pending hearings before the Commission to avoid impairing or frustrating the Court of Appeals' appellate jurisdiction. *FTC v. Dean Foods Co.*, 384 U. S. 514 (1966).

The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice, *Mississippi Valley Barge Line Co. v. United States*, 273 F. Supp. 1, 6 (ED Mo. 1967), summarily aff'd, 389 U. S. 579 (1968); *Board of Education v. York*, 429 F. 2d 66 (CA10 1970), cert. denied, 401 U. S. 954 (1971), and encompasses even those who have not taken any affirmative action to hinder justice. *United States v. McHie*, 196 F. 586 (ND Ill. 1912); *Field v. United States*, 193 F. 2d 92, 95-96 (CA2), cert. denied, 342 U. S. 894 (1951).²⁰

Turning to the facts of this case, we do not think that the Company was a third party so far removed from the underlying controversy that its assistance could not be permissibly compelled. A United States District Court found that there was probable cause to believe that the Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis. For the Company, with this knowledge, to refuse to supply the meager assistance required by the FBI in its efforts to put an end to this venture threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used. Moreover, it can hardly be contended that the Company, a highly regulated public utility with a duty to serve the public,²¹ had a substantial interest in not providing assistance. Certainly the use of pen registers is by no means offensive to it. The Company concedes that it regularly employs such devices without court order for the purposes of checking billing operations, detecting fraud, and

²⁰ See *Labette County Comm'rs v. Moulton*, 112 U. S. 217, 221 (1884): "[I]t does not follow because the jurisdiction in mandamus [now included in § 1651] is ancillary merely that it cannot be exercised over persons not parties to the judgment sought to be enforced."

²¹ See 47 U. S. C. § 201 (a) and N. Y. Pub. Serv. Law § 91 (*McKinney* 1955 and Supp. 1977-1978).

preventing violations of law.²² It also agreed to supply the FBI with all the information required to install its own pen registers. Nor was the District Court's order in any way burdensome. The order provided that the Company be fully reimbursed at prevailing rates, and compliance with it required minimal effort on the part of the Company and no disruption to its operations.

Finally, we note, as the Court of Appeals recognized, that without the Company's assistance there is no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished.²³ The FBI, after an exhaustive search, was unable to find a location where it could install its own pen registers without tipping off the targets of the investigation. The provision of a leased line by the Company was essential to the fulfillment of the purpose—to learn the identities of those connected with the gambling operation—for which the pen register order had been issued.²⁴

²² Tr. of Oral Arg. 27-28, 40.

²³ The dissent's attempt to draw a distinction between orders in aid of a court's own duties and jurisdiction and orders designed to better enable a party to effectuate his rights and duties, *post*, at 189-190, is specious. Courts normally exercise their jurisdiction only in order to protect the legal rights of parties. In *Price v. Johnston*, 334 U. S. 266 (1948), for example, the production of the federal prisoner in court was required in order to enable him to effectively present his appeal which the court had jurisdiction to hear. Similarly, in *Harris v. Nelson*, 394 U. S. 286 (1969), discovery was ordered in connection with a habeas corpus proceeding for the purpose of enabling a prisoner adequately to protect his rights. Here, we have held that Fed. Rule Crim. Proc. 41 provided the District Court with power to authorize the FBI to install pen registers. The order issued by the District Court compelling the Company to provide technical assistance was required to prevent nullification of the court's warrant and the frustration of the Government's right under the warrant to conduct a pen register surveillance, just as the orders issued in *Price* and *Harris* were necessary to protect the rights of prisoners.

²⁴ We are unable to agree with the Company's assertion that "it is extraordinary to expect citizens to directly involve themselves in the law

The order compelling the Company to provide assistance was not only consistent with the Act but also with more recent congressional actions. As established in Part II, *supra*, Congress clearly intended to permit the use of pen registers by federal law enforcement officials. Without the assistance of the Company in circumstances such as those presented here, however, these devices simply cannot be effectively employed. Moreover, Congress provided in a 1970 amendment to Title III that “[a]n order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier . . . shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively” 18 U. S. C. § 2518 (4). In light of this direct

enforcement process.” Tr. of Oral Arg. 41. The conviction that private citizens have a duty to provide assistance to law enforcement officials when it is required is by no means foreign to our traditions, as the Company apparently believes. See *Babington v. Yellow Taxi Corp.*, 250 N. Y. 14, 17, 164 N. E. 726, 727 (1928) (Cardozo, C. J.) (“Still, as in the days of Edward I, the citizenry may be called upon to enforce the justice of the state, not faintly and with lagging steps, but honestly and bravely and with whatever implements and facilities are convenient and at hand”). See also *In re Quarles and Butler*, 158 U. S. 532, 535 (1895) (“It is the duty . . . of every citizen, to assist in prosecuting, and in securing the punishment of, any breach of the peace of the United States”); *Hamilton v. Regents*, 293 U. S. 245, 265 n. (1934) (Cardozo, J., concurring); *Elrod v. Moss*, 278 F. 123, 129 (CA4 1921). The concept that citizens have a duty to assist in enforcement of the laws is at least in part the predicate of Fed. Rule Crim. Proc. 17, which clearly contemplates power in the district courts to issue subpoenas and subpoenas *duces tecum* to nonparty witnesses and to hold noncomplying, nonparty witnesses in contempt. Cf. *Roviaro v. United States*, 353 U. S. 53, 59 (1957) (“The [informer’s] privilege recognizes the obligation of citizens to communicate their knowledge of the commission of crimes to law-enforcement officials and, by preserving their anonymity, encourages them to perform that obligation”). Of course we do not address the question of whether and to what extent such a general duty may be legally enforced in the diverse contexts in which it may arise.

command to federal courts to compel, upon request, any assistance necessary to accomplish an electronic interception, it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy.²⁵ We are convinced that

²⁵ We reject the Court of Appeals' suggestion that the fact that Congress amended Title III to require that communication common carriers provide necessary assistance in connection with electronic surveillance within the scope of Title III reveals a congressional "doubt that the courts possessed inherent power to issue such orders" and therefore "it seems reasonable to conclude that similar authorization should be required in connection with pen register orders . . ." 538 F. 2d, at 962. The amendment was passed following the decision of the Ninth Circuit in *Application of United States*, 427 F. 2d 639 (1970), which held that absent specific statutory authority, a United States District Court was without power to compel a telephone company to assist in a wiretap conducted pursuant to Title III. The court refused to infer such authority in light of Congress' silence in a statute which constituted a "comprehensive legislative treatment" of wiretapping. *Id.*, at 643. We think that Congress' prompt action in amending the Act was not an acceptance of the Ninth Circuit's view but "more in the nature of an overruling of that opinion." *United States v. Illinois Bell Tel. Co.*, 531 F. 2d, at 813. The meager legislative history of the amendment indicates that Congress was only providing an unequivocal statement of its intent under Title III. See 115 Cong. Rec. 37192 (1969) (remarks of Sen. McClellan). We decline to infer from a congressional grant of authority under these circumstances that such authority was previously lacking. See *FTC v. Dean Foods Co.*, 384 U. S. 597, 608-612 (1966); *Wong Yang Sung v. McGrath*, 339 U. S. 33, 47 (1950).

Moreover, even if Congress' action were viewed as indicating acceptance of the Ninth Circuit's view that there was no authority for the issuance of orders compelling telephone companies to provide assistance in connection with wiretaps without an explicit statutory provision, it would not follow that explicit congressional authorization was also needed to order telephone companies to assist in the installation and operation of pen registers which, unlike wiretaps, are not regulated by a comprehensive statutory scheme. In any event, by amending Title III Congress has now required that at the Government's request telephone companies be directed to provide

to prohibit the order challenged here would frustrate the clear indication by Congress that the pen register is a permissible law enforcement tool by enabling a public utility to thwart a judicial determination that its use is required to apprehend and prosecute successfully those employing the utility's facilities to conduct a criminal venture. The contrary judgment of the Court of Appeals is accordingly reversed.

So ordered.

MR. JUSTICE STEWART, concurring in part and dissenting in part.

I agree that the use of pen registers is not governed by the requirements of Title III and that the District Court had authority to issue the order authorizing installation of the pen register, and so join Parts I, II, and III of the Court's opinion. However, I agree with MR. JUSTICE STEVENS that the District Court lacked power to order the telephone company to assist the Government in installing the pen register, and thus join Part II of his dissenting opinion.

MR. JUSTICE STEVENS, with whom MR. JUSTICE BRENNAN and MR. JUSTICE MARSHALL join, dissenting in part.

Today's decision appears to present no radical departure from this Court's prior holdings. It builds upon previous intimations that a federal district court's power to issue a search warrant under Fed. Rule Crim. Proc. 41 is a flexible one, not strictly restrained by statutory authorization, and it applies the same flexible analysis to the All Writs Act, 28 U. S. C. § 1651 (a). But for one who thinks of federal courts as courts of limited jurisdiction, the Court's decision is difficult

assistance in connection with wire interceptions. It is plainly unlikely that Congress intended at the same time to leave federal courts without authority to require assistance in connection with pen registers.

to accept. The principle of limited federal jurisdiction is fundamental; never is it more important than when a federal court purports to authorize and implement the secret invasion of an individual's privacy. Yet that principle was entirely ignored on March 19 and April 2, 1976, when the District Court granted the Government's application for permission to engage in surveillance by means of a pen register, and ordered the respondent to cooperate in the covert operation.

Congress has not given the federal district courts the power either to authorize the use of a pen register, or to require private parties to assist in carrying out such surveillance. Those defects cannot be remedied by a patchwork interpretation of Rule 41 which regards the Rule as applicable as a grant of authority, but inapplicable insofar as it limits the exercise of such authority. Nor can they be corrected by reading the All Writs Act as though it gave federal judges the wide-ranging powers of an ombudsman. The Court's decision may be motivated by a belief that Congress would, if the question were presented to it, authorize both the pen register order and the order directed to the Telephone Company.¹ But the history and consistent interpretation of the federal court's power to issue search warrants conclusively show that, in these areas, the Court's rush to achieve a logical result must await congressional deliberation. From the beginning of our Nation's history, we have sought to prevent the accretion of arbitrary police powers in the federal courts; that accretion is no less dangerous and unprecedented because the first step appears to be only minimally intrusive.

I

Beginning with the Act of July 31, 1789, 1 Stat. 29, 43, and concluding with the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 197, 219, 238, Congress has enacted a

¹ In fact, Congress amended Title III when presented with a similar question. See *ante*, at 177-178, n. 25.

series of over 35 different statutes granting federal judges the power to issue search warrants of one form or another. These statutes have one characteristic in common: they are specific in their grants of authority and in their inclusion of limitations on either the places to be searched, the objects of the search, or the requirements for the issuance of a warrant.² This is not a random coincidence; it is a reflection of a concern deeply imbedded in our revolutionary history for the abuses that attend any broad delegation of power to issue search warrants. In the colonial period, the oppressive British practice of allowing courts to issue "general warrants" or "writs of assistance"³ was one of the major catalysts of the struggle for independence.⁴ After independence, one of the first state constitutions expressly provided that "no warrant ought to be issued but in cases, and with the formalities, prescribed by the laws."⁵ This same principle motivated the adoption of

² The statutes enacted prior to 1945 are catalogued in the Appendix to Mr. Justice Frankfurter's eloquent dissent in *Davis v. United States*, 328 U. S. 582, 616-623.

³ These writs authorized the indiscriminate search and seizure of undescribed persons or property based on mere suspicion. See N. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* 51-55 (1937). The writs of assistance were viewed as particularly oppressive. They commanded "all officers and subjects of the Crown to assist in their execution," and they were not returnable after execution, but rather served as continuous authority during the lifetime of the reigning sovereign. *Id.*, at 53-54.

⁴ The importance of the colonial resistance to general writs and writs of assistance in our history has been emphasized in several Supreme Court cases, e. g., *Frank v. Maryland*, 359 U. S. 360, 363-365; *Henry v. United States*, 361 U. S. 98, 100-101; *Stanford v. Texas*, 379 U. S. 476, 481-485, and is set forth in detail in Lasson, *supra*, and Fraenkel, *Concerning Searches and Seizures*, 34 Harv. L. Rev. 361 (1921).

⁵ Article XIV of the Massachusetts Constitution of 1780. The Fourth Amendment was patterned after this provision. See *Harris v. United States*, 331 U. S. 145, 158 (Frankfurter, J., dissenting).

the Fourth Amendment and the contemporaneous, specific legislation limiting judicial authority to issue search warrants.⁶

It is unnecessary to develop this historical and legislative background at any great length, for even the rough contours make it abundantly clear that federal judges were not intended to have any roving commission to issue search warrants. Quite properly, therefore, the Court today avoids the error committed by the Courts of Appeals which have held that a district court has "inherent power" to authorize the installation of a pen register on a private telephone line.⁷ Federal courts have no such inherent power.⁸

⁶ It was not until 1917 that Congress granted the federal courts, as part of the Espionage Act, broad powers to issue search warrants. 40 Stat. 217, 228 (allowing warrants for stolen property, property used in the commission of a felony, and property used to unlawfully aid a foreign government). These provisions of the Espionage Act formed the basis of Rule 41. See Notes of Advisory Committee on Rules, 18 U. S. C. App., p. 4512. It is clear that the Espionage Act did not delegate authority to issue all warrants compatible with the Fourth Amendment. After the Act, Congress continued to enact legislation authorizing search warrants for particular items, and the courts recognized that, if a warrant was not specifically authorized by the Act—or another congressional enactment—it was prohibited. See *Colyer v. Skeffington*, 265 F. 17, 45 (Mass. 1920), rev'd on other grounds, 277 F. 129 (CA1 1922). See also *Warden v. Hayden*, 387 U. S. 294, 308 n. 12.

⁷ See *United States v. Southwestern Bell Tel. Co.*, 546 F. 2d 243, 245 (CAS 1976); *United States v. Illinois Bell Tel. Co.*, 531 F. 2d 809 (CA7 1976) (*semble*).

⁸ I recognize that there are opinions involving warrantless electronic surveillance which assume that courts have some sort of nonstatutory power to issue search warrants. See *United States v. Giordano*, 416 U. S. 505, 554 (Powell, J., concurring); *Katz v. United States*, 389 U. S. 347; *Osborn v. United States*, 385 U. S. 323. That assumption was not, however, necessary to the decisions in any of those cases, and *Katz* may rest on a reading of Fed. Rule Crim. Proc. 41, see discussion, *infra*, at 184-185. Admittedly, *Osborn* appears to rely in part on a nonstatutory order to permit a secret recording of a conversation with a lawyer who attempted to bribe a witness. But, as the Court subsequently made clear in *United States v. White*, 401 U. S. 745, prior judicial authorization was not a necessary element of that case. Moreover, since the court in *Osborn* was

While the Court's decision eschews the notion of inherent power, its holding that Fed. Rule Crim. Proc. 41 authorizes the District Court's pen register order is equally at odds with the 200-year history of search warrants in this country and ignores the plain meaning and legislative history of the very Rule on which it relies. Under the Court's reading of the Rule, the definition of the term "property" in the Rule places no limits on the objects of a proper search and seizure, but is merely illustrative. *Ante*, at 169. The Court treats Rule 41 as though it were a general authorization for district courts to issue any warrants not otherwise prohibited. *Ante*, at 170. This is a startling approach. On its face, the Rule grants no such open-ended authority. Instead, it follows in the steps of the dozens of enactments that preceded it: It limits the nature of the property that may be seized and the circumstances under which a valid warrant may be obtained. The continuing force of these limitations is demonstrated by the congressional actions which compose the Omnibus Crime Control and Safe Streets Act of 1968.

In Title III of that Act, Congress legislated comprehensively on the subject of wiretapping and electronic surveillance. Specifically, Congress granted federal judges the power to authorize electronic surveillance under certain carefully defined circumstances. As the Court demonstrates in Part II of its opinion (which I join), the installation of pen register devices is not encompassed within that authority. What the majority opinion fails to point out, however, is that in Title IX of that same Act, Congress enacted another, distinct provision extending the power of federal judges to issue search

concerned with the integrity of its own procedures, the argument that it possessed an inherent power to authorize a nonstatutory investigation had far greater strength than it has in the context of an ordinary criminal investigation. Cf. *American Tobacco Co. v. Werckmeister*, 146 F. 375 (CA2 1906), *aff'd*, 207 U. S. 284 (use of All Writs Act to seize goods in the support of the court's jurisdiction).

warrants. That statute, which formed the basis of the 1972 amendment to Rule 41, authorized the issuance of search warrants for an additional class of property, namely, "property that constitutes evidence of a criminal offense in violation of the laws of the United States." 18 U. S. C. § 3103a. In order to understand this provision, it must be remembered that, prior to 1967, "mere evidence" could not be the subject of a constitutionally valid seizure. *Gouled v. United States*, 255 U. S. 298. In *Warden v. Hayden*, 387 U. S. 294, this Court removed the constitutional objection to mere-evidence seizures. Title IX was considered necessary because, after *Warden v. Hayden*, there existed a category of property—mere evidence—which could be the subject of a valid seizure incident to an arrest, but which could not be seized pursuant to a warrant. The reason mere evidence could not be seized pursuant to a warrant was that, as Congress recognized, Rule 41 did not authorize warrants for evidence.⁹ Title IX was enacted to fill this gap in the law.¹⁰

⁹ In the edition of his treatise written after the decision in *Warden v. Hayden* in 1967 and prior to the 1972 amendment to Rule 41, Professor Wright acutely observed:

"Immediately after the Hayden decision there was an apparent anomaly, since the case held that evidence might be seized, but Rule 41 (b) did not authorize issuance of a search warrant for evidence. This would have meant that evidence might be seized where a search may permissibly be made without a warrant, but not in a search under warrant. This would have been wholly inconsistent with the strongly-held notion that, save in a few special classes of cases, a warrant should be a prerequisite to a search, and it would have encouraged police to search without a warrant. Congress, which can move more quickly than the rulemaking apparatus, responded by passage of a statute making it permissible to issue a search warrant for 'property that constitutes evidence of a criminal offense in violation of the laws of the United States.' This supplements, and may well soon swallow up, the other grounds for a search warrant set out in Rule 41 (b)." (Footnotes omitted.) 3 C. Wright, *Federal Practice and Procedure* § 664 (1969).

¹⁰ See comments of Senator Allott, who introduced Title IX in the Senate, 114 Cong. Rec. 14790 (1968).

Two conclusions follow ineluctably from the congressional enactment of Title IX. First, Rule 41 was never intended to be a general authorization to issue any warrant not otherwise prohibited by the Fourth Amendment. If it had been, Congress would not have perceived a need to enact Title IX, since constitutional law, as it stood in 1968, did not prohibit the issuance of warrants for evidence.¹¹

Second, the enactment of Title IX disproves the theory that the definition of "property" in Rule 41 (h) is only illustrative. This suggestion was first put forward by the Court in *Katz v. United States*, 389 U. S. 347. The issue was not briefed in *Katz*, but the Court, in dicta, indicated that Rule 41 was not confined to tangible property. Whatever the merits of that suggestion in 1967, it has absolutely no force at this time. In 1968 Congress comprehensively dealt with the issue of electronic searches in Title III. In the same Act, it provided authority for expanding the scope of property covered under Rule 41. But the definition of property in the Rule has never changed. Each item listed is tangible,¹² and the final reference to "and any other tangible items" surely must now be read as describing the outer limits of the included category.¹³ It strains

¹¹ Indeed, under the Court's flexible interpretation of Rule 41, the entire series of statutes that belie the "inherent power" concept, was also an exercise in futility because the silence of Congress would not have prohibited any warrant that did not violate the Fourth Amendment. Many of these statutes remain in effect, *e. g.*, 49 U. S. C. § 782 (seizure of certain contraband); 19 U. S. C. § 1595 (customs duties; searches and seizures); and Rule 41 (h) expressly provides that Rule 41 "does not modify any act, inconsistent with it, regulating search, seizure and the issuance and execution of search warrants"

¹² Rule 41 (h) provides in part:

"The term 'property' is used in this rule to include documents, books, papers and any other tangible objects."

¹³ The Court acknowledges that the amendment to Rule 41 (b) eliminated a "restriction" against the seizure of mere evidence. *Ante*, at 170-171, n. 18. What the Court refers to as a "restriction" was nothing more than silence—the absence of an express grant of authority. Since the

credulity to suggest that Congress, having carefully circumscribed the use of electronic surveillance in Title III, would then, in Title IX, expand judicial authority to issue warrants for the electronic seizure of "intangibles" without the safeguards of Title III.¹⁴ In fact, the safeguards contained in Rule 41 make it absurd to suppose that its draftsmen thought they were authorizing any form of electronic surveillance. The paragraphs relating to issuance of the warrant, Rule 41 (c), the preparation of an inventory of property in the presence of the person whose property has been taken, Rule 41 (d), and the motion for a return of property, Rule 41 (e), are almost meaningless if read as relating to electronic surveillance of any kind.

To reach its result in this case, the Court has had to overlook

Rule is just as silent on the subject of seizing intangibles as it was on the subject of seizing mere evidence, it is difficult to understand why the Court does not recognize the same "restriction" against such seizures.

¹⁴ The Court argues that it "would be anomalous to permit the recording of conversations by means of electronic surveillance while prohibiting the far lesser intrusion accomplished by pen registers." *Ante*, at 170. But respondent does not claim that *Congress* has prohibited the use of pen registers. Admittedly there is now no statute either permitting or prohibiting the use of such devices. If that use is a "search" within the meaning of the Fourth Amendment—a question the Court does not decide—there is nothing anomalous about concluding that it is a forbidden activity until Congress has prescribed the safeguards that should accompany any warrant to engage in it. Even if an anomaly does exist, it should be cured by Congress rather than by a loose interpretation of "property" under Rule 41 which may tolerate sophisticated electronic surveillance techniques never considered by Congress and presenting far greater dangers of intrusion than pen registers. See *Michigan Bell Tel. Co. v. United States*, 565 F. 2d 385 (CA6 1977) (indicating the increasing sophistication of surveillance techniques similar to pen registers); cf. *United States v. Pretzinger*, 542 F. 2d 517 (CA9 1976) (use of electronic tracking devices). It is significant that Title III limits the types of criminal investigations for which electronic surveillance may be used; no such limit is expressed in Rule 41 or is implicit in the Court's reasoning today.

the Rule's specific language, its specific safeguards, and its legislative background. This is an extraordinary judicial effort in such a sensitive area, and I can only regard it as most unwise. It may be that a pen register is less intrusive than other forms of electronic surveillance. Congress evidently thought so. See S. Rep. No. 1097, 90th Cong., 2d Sess., 90 (1968). But the Court should not try to leap from that assumption to the conclusion that the District Court's order here is covered by Rule 41. As I view this case, it is immaterial whether or not the attachment of a pen register to a private telephone line is a violation of the Fourth Amendment. If, on the one hand, the individual's privacy interest is not constitutionally protected, judicial intervention is both unnecessary and unauthorized. If, on the other hand, the constitutional protection is applicable, the focus of inquiry should not be whether Congress has prohibited the intrusion, but whether Congress has expressly authorized it, and no such authorization can be drawn from Rule 41. On either hypothesis, the order entered by the District Court on March 19, 1976, authorizing the installation of a pen register, was a nullity. It cannot, therefore, support the further order requiring the New York Telephone Company to aid in the installation of the device.

II

Even if I were to assume that the pen register order in this case was valid, I could not accept the Court's conclusion that the District Court had the power under the All Writs Act, 28 U. S. C. § 1651 (a), to require the New York Telephone Company to assist in its installation. This conclusion is unsupported by the history, the language, or previous judicial interpretations of the Act.

The All Writs Act was originally enacted, in part, as § 14 of the Judiciary Act of 1789, 1 Stat. 81.¹⁵ The Act was, and

¹⁵ The statute was also derived from § 13 of the Judiciary Act, which concerned writs of mandamus and prohibition, 1 Stat. 80, and a statute

is, necessary because federal courts are courts of limited jurisdiction having only those powers expressly granted by Congress,¹⁶ and the statute provides these courts with the procedural tools—the various historic common-law writs—necessary for them to exercise their limited jurisdiction.¹⁷ The statute does not contain, and has never before been interpreted as containing, the open-ended grant of authority to federal courts that today's decision purports to uncover. Instead, in the language of the statute itself, there are two fundamental limitations on its scope. The *purpose* of any order authorized by the Act must be to aid the court in the exercise of its jurisdiction;¹⁸ and the *means* selected must be analogous to a common-law writ. The Court's opinion ignores both limitations.

dealing with writs of *ne exeat*, 1 Stat. 334. The All Writs Act now reads:

"(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."

¹⁶ This proposition was so well settled by 1807 that Mr. Chief Justice Marshall needed no citation to support the following statement:

"As preliminary to any investigation of the merits of this motion, this court deems it proper to declare that it disclaims all jurisdiction not given by the constitution, or by the laws of the United States.

"Courts which originate in the common law possess a jurisdiction which must be regulated by their common law, until some statute shall change their established principles; but courts which are created by written law, and whose jurisdiction is defined by written law, cannot transcend that jurisdiction. It is unnecessary to state the reasoning on which this opinion is founded, because it has been repeatedly given by this court; and with the decisions heretofore rendered on this point, no member of the bench has, even for an instant, been dissatisfied." *Ex parte Bollman*, 4 Cranch 75, 93.

¹⁷ See *Harris v. Nelson*, 394 U. S. 286, 299.

¹⁸ This Court has frequently considered this requirement in the context of orders necessary or appropriate in the exercise of appellate jurisdiction. See J. Moore, B. Ward, & J. Lucas, 9 *Moore's Federal Practice* ¶¶ 110.27–110.28 (1975). Here, we are faced with an order that must be necessary or appropriate in the exercise of a district court's original jurisdiction.

The Court starts from the premise that a district court may issue a writ under the Act "to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained." *Ante*, at 172. As stated, this premise is neither objectionable nor remarkable and conforms to the principle that the Act was intended to aid the court in the exercise of its jurisdiction. Clearly, if parties were free to ignore a court judgment or order, the court's ability to perform its duties would be undermined. And the court's power to issue an order requiring a party to carry out the terms of the original judgment is well settled. See *Root v. Woolworth*, 150 U. S. 401, 410-413. The courts have also recognized, however, that this power is subject to certain restraints. For instance, the relief granted by the writ may not be "of a different kind" or "on a different principle" from that accorded by the underlying order or judgment. See *id.*, at 411-412.¹⁹

¹⁹ These restraints are necessary concomitants of the undisputed fact that the All Writs Act does not provide federal courts with an independent grant of jurisdiction. *McIntire v. Wood*, 7 Cranch 504; *Rosenbaum v. Bauer*, 120 U. S. 450. The factors mentioned above may be relevant in determining whether the court has ancillary jurisdiction over the dispute. See *Dugas v. American Surety Co.*, 300 U. S. 414; *Labette County Commr's v. Moulton*, 112 U. S. 217; *Morrow v. District of Columbia*, 135 U. S. App. D. C. 160, 417 F. 2d 728 (1969). In this case, the District Court's order was entered against a third party—the Telephone Company. The Court never explains on what basis the District Court had jurisdiction to enter this order. Possibly, the District Court believed that it had ancillary jurisdiction over the controversy, or that the failure of the Company to aid the Government posed a federal question under 28 U. S. C. § 1331. See *Board of Education v. York*, 429 F. 2d 66 (CA10 1970), cert. denied, 401 U. S. 954. Since I believe that the District Court could not enter its order in any event since it was not in aid of its jurisdiction, I do not find it necessary to reach the question whether there was jurisdiction, apart from the All Writs Act, over the "dispute" between the Government and the Telephone Company. However, the Court's failure to indicate the basis of jurisdiction is inexplicable.

More significantly, the courts have consistently recognized and applied the limitation that whatever action the court takes must be in aid of *its* duties and *its* jurisdiction.²⁰ The fact that a party may be better able to effectuate its rights or duties if a writ is issued never has been, and under the language of the statute cannot be, a sufficient basis for issuance of the writ. See *Sampson v. Murray*, 415 U. S. 61; *Commercial Security Bank v. Walker Bank & Trust Co.*, 456 F. 2d 1352 (CA10, 1972); J. Moore, B. Ward, & J. Lucas, 9 Moore's Federal Practice ¶ 110.29 (1975).

Nowhere in the Court's decision or in the decisions of the lower courts is there the slightest indication of why a writ is necessary or appropriate in this case to aid the District Court's jurisdiction. According to the Court, the writ is necessary because the Company's refusal "threatened obstruc-

²⁰ The Court's failure to explain why the District Court's order was in aid of its jurisdiction is particularly notable when compared to the rationale of the prior Court cases on which it relies. See, e. g., *Harris v. Nelson*, 394 U. S. 286, 299 ("the habeas corpus jurisdiction and the duty to exercise it being present, the courts may fashion appropriate modes of procedure Where their duties require it, this is the inescapable obligation of the courts") (emphasis added); *FTC v. Dean Foods Co.*, 384 U. S. 597, 604 (injunction issued under All Writs Act upheld because it was necessary "to preserve the *status quo* while administrative proceedings are in progress and prevent impairment of the effective exercise of appellate jurisdiction") (emphasis added).

The Court apparently concludes that there is no functional distinction between orders designed to enable a party to effectuate its rights and orders necessary to aid a court in the exercise of its jurisdiction. *Ante*, at 175 n. 23. The Court reaches this conclusion by pointing out that the orders in cases such as *Harris v. Nelson*, *supra*, protected a party's rights. This is, of course, true. Orders in aid of a court's jurisdiction will usually be beneficial to one of the parties before the court. The converse, however, is clearly not true. Not all orders that may enable a party to effectuate its rights aid the court in its exercise of jurisdiction. Compare *Sampson v. Murray*, 415 U. S. 61, with *FTC v. Dean Foods Co.*, *supra*.

tion of an investigation” *Ante*, at 174. Concededly, citizen cooperation is always a desired element in any government investigation, and lack of cooperation may thwart such an investigation, even though it is legitimate and judicially sanctioned.²¹ But unless the Court is of the opinion that the District Court’s interest in its jurisdiction was coextensive with the Government’s interest in a successful investigation, there is simply no basis for concluding that the inability of the Government to achieve the purposes for which it obtained the pen register order in any way detracted from or threatened the District Court’s jurisdiction. Plainly, the District Court’s jurisdiction does not ride on the Government’s shoulders until successful completion of an electronic surveillance.

If the All Writs Act confers authority to order persons to aid the Government in the performance of its duties, and is no longer to be confined to orders which must be entered to enable the court to carry out its functions, it provides a sweeping grant of authority entirely without precedent in our Nation’s history. Of course, there is precedent for such authority in the common law—the writ of assistance. The use of that writ by the judges appointed by King George III was one British practice that the Revolution was specifically intended to terminate. See n. 3, *supra*. I can understand why the Court today does not seek to support its holding by reference to that writ, but I cannot understand its disregard of the statutory requirement that the writ be “agreeable to the usages and principles of law.”

²¹ A citizen is not, however, free to forcibly prevent the execution of a search warrant. Title 18 U. S. C. § 2231 imposes criminal penalties on any person who “forcibly assaults, resists, opposes, prevents, impedes, intimidates, or interferes with any person authorized to serve or execute search warrants” This section was originally enacted as part of the Espionage Act of 1917, see n. 6, *supra*, and is the only statutory provision imposing any duty on the general citizenry to “assist” in the execution of a warrant.

III

The order directed against the Company in this case is not particularly offensive. Indeed, the Company probably welcomes its defeat since it will make a normal profit out of compliance with orders of this kind in the future. Nevertheless, the order is deeply troubling as a portent of the powers that future courts may find lurking in the arcane language of Rule 41 and the All Writs Act.

I would affirm the judgment of the Court of Appeals.

114 (1952), has clearly held in an extradition situation that a fugitive from justice must challenge the constitutionality of his (or her) incarceration in the demanding state and not in the asylum state. The sparse law in this circuit has followed the Supreme Court mandate. *United States ex rel. Hammershoy v. Director of Conn. Corr. Ctr.*, 299 F.Supp. 1354, 1356 (D.Conn.1969) (Timbers, Ch. J.). *Hammershoy* recognized the possibility of a contrary rule on a showing of "very unusual facts," *id.*, presumably referring to the arguable intimation in *Sweeney* that such might be the result on a showing that relief is unavailable in the courts of the demanding state.

There is, however, no basis on which to conclude that the courts of the State of North Carolina would be unable to afford petitioner her relief, notwithstanding a vague suggestion in the petition to the contrary. Indeed, the fact that Ms. Little was acquitted on the murder charge in a North Carolina court would belie such a suggestion. Should there be any failure on the part of the North Carolina state courts to accept and apply the requirements of the Constitution of the United States, relief in the federal court sitting in the State of North Carolina is available.

To me the law is clear. It requires that the petition for the writ of habeas corpus be dismissed. At the hearing, the attorney for the petitioner requested a stay pending appeal in the event of an adverse determination. Since I believe that there is no probable cause for an appeal, I will not issue either the required certificate of probable cause (28 U.S.C. § 2253) or a stay.

SO ORDERED.



Freddie Joe SIMMONS, Plaintiff,

v.

SOUTHWESTERN BELL TELEPHONE COMPANY, a corporation, Defendant.

No. CIV-77-0487-T.

United States District Court,
W. D. Oklahoma.

May 19, 1978.

Former employee of telephone company sued company alleging that its actions in monitoring his private telephone conversations were unlawful and unconstitutional. On defendant's motion for summary judgment, the District Court, Thompson, J., held that: (1) where telephone company maintained a "testdesk" where trouble reports from customers were handled, and use of testdesk telephone by employees was monitored by supervisors for quality control and other purposes, and where employee knew that personal calls were not be made from the testdesk and that his telephone conversations from the desk could be and were monitored, he could not recover against telephone company on ground that monitoring his private conversations on the testdesk telephone violated constitutional right of privacy; (2) company's monitoring activities fell within exception from prohibition against intercepting wire communications contained in the Omnibus Crime Control and Safe Streets Act of 1968; (3) since company lawfully monitored plaintiff's phone calls, any disclosure thereof was not a violation of the Act, and (4) section of the Communications Act of 1934 prohibiting unauthorized publication or use of communications exempts from its coverage those activities authorized by the 1968 Act.

Motion granted.

1. Constitutional Law ¶82(7)

Whatever the source of constitutional right of privacy, the protection is only against government intrusion into a person's privacy, and it protects only a reason-

SIMMONS v. SOUTHWESTERN BELL TEL. CO.

393

Cite as 452 F.Supp. 392 (1978)

expectation of privacy. U.S.C.A. Const. Amends. 1, 4, 5, 9, 14.

1. Torts ⇐ 8.5(2)

Where telephone company maintained "testdesk" where trouble reports from customers were handled, and use of test-telephone by employees was monitored by supervisors for quality control and other purposes, and where employee knew that personal calls were not to be made from the testdesk and that his telephone conversations from the desk could be and were monitored, he could not recover against telephone company on ground that monitoring of private conversations on the testdesk telephone violated constitutional right of privacy, since the company was not an arm of the government nor responsible under Fourth Amendment as a government agency, and since, in any event, employee did not have a reasonable expectation under the circumstances that he could protect his personal conversations from intrusion. U.S. Const. Amends. 4, 9.

2. Telecommunications ⇐ 491

Where telephone company maintained testboard where trouble reports from customers were handled and use of board by employees was monitored by supervisors for purpose of service quality control checks and, in plaintiff employee's case, for purpose of preventing his persistent use of testboard phone for personal calls, against which he had been warned several times, company's legitimate interest in maintaining quality control and availability of lines outweighs its monitoring activities within exception from prohibition against interception of wire communications, contained in Omnibus Crime Control and Safe Streets Act of 1968. 18 U.S.C.A. §§ 2511, 2511(2)(a)(i), 2520.

4. Telecommunications ⇐ 491

Where telephone company lawfully monitored employee's telephone calls at "test-

1. Deposition of plaintiff, pp. 25-27.

2. Affidavit of Dennis J. Fowler, Exhibit A, defendant's brief in support of the Motion for Summary Judgment.

desk," within meaning of the Omnibus Crime Control and Safe Streets Act of 1968, any disclosure of such conversations was not a violation of the Act since disclosure, to be unlawful thereunder, must be of information which was unlawfully intercepted. 18 U.S.C.A. §§ 2511, 2511(2)(a)(i), 2520.

5. Telecommunications ⇐ 492

Section of the Communications Act of 1934 prohibiting unauthorized publication or use of communications exempts from its coverage those activities authorized by the Omnibus Crime Control and Safe Streets Act of 1968. 18 U.S.C.A. § 2510 et seq.; Communications Act of 1934, § 605, 47 U.S.C.A. § 605.

Lyle McPheeters, Oklahoma City, Okl., for plaintiff.

Thomas J. Enis and Robert D. Allen, Oklahoma City, Okl., for defendant.

MEMORANDUM OPINION

THOMPSON, District Judge.

Plaintiff herein was formerly employed by defendant at its test center in Oklahoma City. His job, at the time of the acts complained of herein, was that of "deskman" or "testboardman". As such, plaintiff was one of several employees at a "testdesk"—a large and complex panel where all trouble reports from customers were received, cleared, dispatched, and closed.¹ The supervisors, or chief deskmen, monitored the use of testboard telephones for service quality checks, checking work in progress, assisting deskmen, and insuring minimum use of customer monitoring by deskmen.² The deskmen, and specifically plaintiff, knew that the testboard lines were monitored.³ It was the written policy of defendant, and understood by plaintiff, that personal calls made to or from the testboard were not allowed.⁴

3. Deposition of plaintiff, pp. 94, 99.

4. Deposition of plaintiff, Exhibit 1.

There were other telephones, not subject to service observing, available for personal calls.⁵ Plaintiff had been warned repeatedly against his excessive use of the testboard phones for private calls.⁶ In this action plaintiff alleges that the actions of defendant in monitoring his private conversations on the testboard telephones were unlawful, unconstitutional, and caused him damages exceeding \$6,000,000.

Plaintiff brings this action on two separate theories of recovery—he alleges first a violation of his constitutional right to privacy, and secondly, a violation of 18 U.S.C. §§ 2510, et seq., entitling him to a private right of damages. He seeks actual and punitive damages as a result of the defendant's actions, including his allegedly wrongful termination from employment. Defendant has moved for summary judgment, which motion has been briefed by the parties and is ready for decision. Plaintiff has, during the time for briefing this motion, applied for and obtained leave to amend his complaint. Defendant has asked that its Motion for Summary Judgment be directed to the amended complaint, as the cause of action is essentially the same. Thus the Court has read the briefs of the parties on the Motion for Summary Judgment as be-

ing directed to plaintiff's second amended complaint.

Constitutional Right to Privacy

[1, 2] The constitutional protection of the right to privacy is a relatively new development in our law,⁷ but with historical precedent.⁸ The right to privacy has been found under the First,⁹ Fourth,¹⁰ Fifth,¹¹ Ninth,¹² and Fourteenth Amendments,¹³ and the "penumbra of the Bill of Rights".¹⁴ It is clear that, whatever the source of the right, the protection is only as against government intrusions into a person's privacy.¹⁵ The defendant herein is certainly not an arm of the government and is not "responsible under the Fourth Amendment as [a] government bod[y]".¹⁶

Moreover, as the law in this area continually evolves and becomes more concrete, it is inevitable that the right protected is not absolute and unequivocal, but rather that the Constitution protects only a *reasonable expectation of privacy*.¹⁷ Plaintiff herein was well aware that his telephone conversations could be monitored, and in fact were. It is not a "reasonable expectation" under these circumstances that plaintiff could protect his personal conversations from intrusion.

5. Affidavit of Dennis J. Fowler, *supra*. n. 2; deposition of plaintiff, p. 94.

6. Deposition of plaintiff, pp. 97, 98.

7. See, e. g., *Katz v. U. S.*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Griswold v. Connecticut*, 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965); *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961).

8. *Union Pacific R. Co. v. Botsford*, 141 U.S. 250, 11 S.Ct. 1000, 35 L.Ed. 734 (1891); *Boyd v. U. S.*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886).

9. *Stanley v. Georgia*, 394 U.S. 557, 564, 89 S.Ct. 1243 (1960); *NAACP v. Alabama*, 357 U.S. 449, 462, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958).

10. *Katz v. U. S.*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Mapp v. Ohio*, 367 U.S. 643, 81 S.Ct. 1684, 6 L.Ed.2d 1081 (1961).

11. *Boyd v. U. S.*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886).

12. *Griswold v. Connecticut*, 381 U.S. 479, 486, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965) (Goldberg, J., concurring).

13. *Id.*, at 499 and 502, 85 S.Ct. 1678 (Harlan, J., and White, J., separate concurring opinions).

14. *Id.*, at 479, 85 S.Ct. 1678 (opinion of Court per Douglas, J.).

15. *Griswold v. Connecticut*, 381 U.S. 479, 483, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965); *Katz v. U. S.*, 389 U.S. 347, 350, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Boyd v. U. S.*, 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746; *U. S. v. Clegg*, 509 F.2d 605 (5th Cir. 1975).

16. *U. S. v. Goldstein*, 532 F.2d 1305, 1311 (9th Cir. 1976), cert. denied sub nom. *Roberts v. U. S.*, 429 U.S. 960, 97 S.Ct. 384, 50 L.Ed.2d 327.

17. *Katz v. U. S.*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *U. S. v. Pui Kan Lam*, 483 F.2d 1202 (2nd Cir. 1973), cert. denied 415 U.S. 984, 94 S.Ct. 1578, 39 L.Ed.2d 881.

Cite as 452 F.Supp. 392 (1978)

The Court takes note of the case of *United States v. Perkins*, 383 F.Supp. 922, 927 (N.D. Ohio 1974), cited and relied on by plaintiff, where the Court stated:

"The Fourth Amendment does not protect unreasonable *governmental* searches only but against *all* unreasonable searches." [Emphasis in original]

This case is inapposite for several reasons. First, the factual setting in *Perkins* was a criminal prosecution where defendant Perkins urged the unconstitutionality of 18 U.S.C. § 2511, as a governmental restriction of private action. It was in this context, i. e., in holding that Congress could legislate against private telephone interception, that the sentence quoted above was expressed. Certainly the Court in *Perkins* did not intend authorization of a constitutional right of action against a private, as opposed to a governmental, body by the quoted statement. Such a result would fly in the face of well-established precedent¹⁸ and would revolutionize long-held concepts of constitutional law.¹⁹ If such was the intent of *Perkins*, it is rejected here. But even accepting that *Perkins* allows a right of relief against non-governmental invasions of privacy, it is inapplicable here, as *Perkins* specifically says the protection is not against "unreasonable *governmental* searches only but against *all* unreasonable searches". The Court defined "unreasonable searches" as those against a person who has an expectation of privacy which must be protected. Plaintiff herein had no such expectation.

Nor can plaintiff find relief in the Ninth Amendment as an authorization of this suit. There is some authority that the Ninth Amendment is the constitutional basis for the protection of privacy, not found specifically in other Amendments.²⁰ Whatever the source of the right (which source seems to be an argument more of semantics than of substance), the right may be asserted, at

18. See authorities cited at n. 15.

19. Such a construction would elevate almost every lawsuit to a constitutional claim, e. g., a conversion becomes an unreasonable seizure, an assault becomes cruel and unusual punishment, false imprisonment becomes an abrogation of freedom to associate, and so on, ad

least in a constitutional context, only against a governmental intrusion, and only where there exists a reasonable expectation of privacy, neither of which exist in the case at hand.

It is the conclusion of the Court that plaintiff has failed to state a claim amounting to a violation of constitutionally protected rights.

18 U.S.C. § 2511

[3] As part of the Omnibus Crime Control and Safe Streets Act of 1968, Congress enacted a prohibition of wire interception and interception of oral communications, 18 U.S.C. §§ 2510, et seq., and provided a private right of action for violations thereof. 18 U.S.C. § 2520. Plaintiff claims that defendant has violated section 2511, which reads in part:

"(1) Except as otherwise specifically provided in this chapter any person who—
(a) wilfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire or oral communication;

shall be fined not more than \$10,000 or imprisoned not more than five years, or both."

Defendant claims it falls within the exception found at section 2511(2)(a)(i):

"It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or

infinitem. Thus all these lawsuits become federal claims and find themselves in federal, rather than state, court.

20. *Griswold v. Connecticut*, 381 U.S. 479, 486, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965), (Goldberg, J., concurring).

property of the carrier of such communication"

This section has so far been tested only as it relates to the propriety of the telephone company's interception of private conversations in order to prevent fraud against the telephone company.²¹ Thus, where the company reasonably suspects the use of a "blue box" to avoid long distance charges, it may lawfully monitor conversations to uncover the fraud. Plaintiff argues that these cases stand for the proposition that defendant may intercept wire communications only to protect itself from fraud against its property and economic interests. Such a construction ignores the language of section 2511(2)(a)(i)—" . . . while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier" (emphasis added). The fact that there are no cases construing the first of the lawful reasons for wire interception by a communications carrier does not mean that the statutory language is of no effect. The Court must give effect to each provision contained in a statute,²² not just the portion that has been previously ruled upon.

Plaintiff does not appear to object, either now or during his employment, to defendant's monitoring of his business calls²³—it is only his personal calls he feels should remain private. It is the assertion of defendant, and admitted by plaintiff,²⁴ however, that there was a telephone available for private calls, and that all employees of defendant were aware of its availability. Had plaintiff been monitored on that telephone, the Court would wholeheartedly agree that defendant had overstepped its limited privilege. However, the record reflects that plaintiff was employed in a complex area involving defendant's quality control. He and fellow employees at the test-

board were in a sensitive and responsible position requiring immediate attention and action and where availability of both incoming and outgoing lines was of paramount importance. Defendant's monitoring activities must be considered reasonable, when the nature of plaintiff's employment is considered with the fact that all employees at his station knew, and had acquiesced to, defendant's monitoring of their incoming and outgoing calls, while at the testboard, both for the purpose of service quality control checks and, in plaintiff's case, for the purpose of preventing his persistent use of the testboard phones for personal calls, a practice against which plaintiff had been warned several times. As plaintiff knew his calls were monitored, he had no reasonable expectation that his calls would remain private; as the defendant had a legitimate interest in maintaining quality control, its monitoring activities fall within the exclusion of 18 U.S.C. § 2511(2)(a)(i).

[4] Plaintiff argues that the actions of a certain employee of defendant in publicly repeating portions of plaintiff's private phone calls were undoubtedly beyond the limited scope of section 2511(2)(a)(i). For the purposes of the motion, the Court has accepted plaintiff's allegations of fact upon which his argument is based as true. Even so assuming, plaintiff states no claim. As the Court has found that defendant lawfully monitored plaintiff's phone calls within the meaning of section 2511(2)(a)(i), any disclosure of such conversations is not a violation of section 2511. Both section 2511 and section 2520, which authorizes a civil damage suit, treat disclosure as a separate offense from interception. Disclosure, to be unlawful under section 2511, must be of information which was unlawfully intercepted:

"Except as otherwise specifically provided in this chapter any person who—

21. *U. S. v. Goldstein*, 532 F.2d 1305 (9th Cir. 1976); *U. S. v. Clegg*, 509 F.2d 605 (5th Cir. 1975); *U. S. v. DeLeeuw*, 368 F.Supp. 426 (D.Wis.1974).

22. *U. S. v. Powers*, 307 U.S. 214, 59 S.Ct. 805, 83 L.Ed. 1245 (1930).

23. Deposition of plaintiff, p. 63.

24. Deposition of plaintiff, p. 94.

TURNER v. WYRICK

397

Cite as 452 F.Supp. 397 (1978)

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication *in violation of this subsection*” [Emphasis added]

Section 2520 allows a private right to damages for “[a]ny person whose wire or oral communication is intercepted, disclosed, or used *in violation of this chapter*” (emphasis added). Thus, having held above that the interception of plaintiff’s telephone conversation was lawful, the Court cannot find a disclosure violation. Plaintiff’s claim that defendant violated section 2511, entitling him to damages under section 2520, is therefore without merit.

47 U.S.C. § 605

[5] Plaintiff asserts that 47 U.S.C. § 605, prohibiting unauthorized publication or use of communications, grants him a cause of action for damages for its violation. The cases cited by plaintiff in support of this proposition predate the 1968 amendment to this section, which added the introductory phrase, “except as authorized by chapter 119, Title 18”. Chapter 119 of Title 18 is sections 2510, et seq., discussed above. At least one court has held, since this amendment, that section 605 does not grant a civil remedy for violations thereunder.²⁵ In any event, section 605 clearly exempts from its coverage those activities authorized by sections 2510, et seq. As the Court has found defendant’s activities lawful within the exception in section 2511(2)(a)(i), section 605 has no application to this suit.

Conclusion

Plaintiff argues that there are questions of fact present in this lawsuit which require a jury determination. The Court can find none. It is the application of law to the

admitted facts which results in a judgment for defendant. Although plaintiff, in his deposition, has alleged that defendant has monitored his home telephone to the present time, such allegations are not part of plaintiff’s second amended complaint and thus are not relevant here. Plaintiff’s allegations of wrongful discharge, plead only as an item of damage from defendant’s monitoring activities, are likewise irrelevant, once the monitoring is found lawful. It is the conclusion of the Court that there is no constitutional protection of non-governmental invasions of privacy; that defendant’s conduct is within both the letter and the spirit of the limited Congressional authorization of telephone interceptions found at 18 U.S.C. § 2511(2)(a)(i); and that defendant’s activity, lawful within section 2511, is lawful within 47 U.S.C. § 605.

Finding no substantial question as to any material fact, the Court finds that defendant is entitled to judgment as a matter of law. Defendant’s Motion for Summary Judgment is therefore granted. A judgment in accordance with the foregoing will be entered this date.



James TURNER, Jr., Petitioner,

v.

Warden Donald W. WYRICK,
Respondent.

No. 77-330C(3).

United States District Court,
E. D. Missouri, E. D.

May 22, 1978.

Plaintiff argues that there are questions of fact present in this lawsuit which require a jury determination. The Court can find none. It is the application of law to the

Missouri prisoner filed a petition for a writ of habeas corpus. The District Court,

25. *Smith v. Cincinnati Post & Times-Star*, 353 F.Supp. 1126 (S.D. Ohio 1972), *aff'd* 475 F.2d 740 (6 Cir.).

UNITED STATES v. HALL

193

Cite as 488 F.2d 193 (1973)

as at trial, presumably he was able to testify from first-hand information.

Were we to hold that grand jury minutes must be turned over so that defense counsel could satisfy his mere suspicion that the indictment was based on insufficient evidence, grand jury proceedings would effectively be open at the whim of the defense. This we are not disposed to do.

Affirmed.



UNITED STATES of America,
Plaintiff-Appellee,

v.

John Merrill HALL, Defendant-Appellant.

UNITED STATES of America,
Plaintiff-Appellee,

v.

William King NICHOLS, Defendant-Appellant.

UNITED STATES of America,
Plaintiff-Appellee,

v.

James Kline DEVER, Defendant-Appellant.

Nos. 72-1841, 72-1842, 72-1737.

United States Court of Appeals,
Ninth Circuit.

Oct. 19, 1973.

Defendants were convicted, in the United States District Court for the District of Arizona, James A. Walsh, J., of possession of marijuana with intent to distribute in violation of statute and conspiracy to commit that offense, and they appealed. The Court of Appeals, Wallace, Circuit Judge, held that 1968 amendment made it obvious that legislature wanted law enforcement personnel to be governed exclusively by the Crime

Control Act, and therefore the statute forbidding any person to intercept and divulge wire or radio communications offered no impediment to application of evidence-excluding rule applicable when non-FCC governmental agents or private individuals intercept nonpublic broadcast without consent.

Reversed and remanded.

Ferguson, District Judge, dissented in part, with an opinion.

1. Searches and Seizures ⇨1

Use of electronic devices to overhear conversation is "search" within Fourth Amendment. U.S.C.A.Const. Amend. 4.

2. Criminal Law ⇨394.2(2)

That state officers had made searches and arrests and then turned case over to federal authorities for prosecution did not prevent raising of question as to validity of searches.

3. Telecommunications ⇨495

A law enforcement officer is not a "person" within statute forbidding divulgence of restricted communications to any person, and it was therefore questionable whether communications by housewife to Arizona Department of Public Safety of contents of conversation overheard on radio violated statute. Communications Act of 1934, § 605 as amended 47 U.S.C.A. § 605.

See publication Words and Phrases for other judicial constructions and definitions.

4. Telecommunications ⇨495

1968 amendment made it obvious that legislature wanted law enforcement personnel to be governed exclusively by the Crime Control Act, and therefore the statute forbidding any person to intercept and divulge wire or radio communications offered no impediment to application of evidence-excluding rule applicable when non-FCC governmental agents or private individuals intercept nonpublic broadcast without consent. Communications Act of 1934, § 605 as amended 47 U.S.C.A. § 605.

5. Telecommunications ⇨493, 496

Congress did not intend that every conversation aided in any part by any wire should be deemed a "wire communication," but when part of communication is carried to or from a land-line telephone, entire conversation is a wire communication and search warrant is required. 18 U.S.C.A. § 2510(1, 2).

See publication Words and Phrases for other judicial constructions and definitions.

6. Constitutional Law ⇨70.1(7)
Telecommunications ⇨493

Logically, conversations intercepted by ordinary radio receiver and not by telephone tap should be afforded no more protection than those occurring between two radio transceivers, but congressional definition required that classification of conversation between mobile and land-line telephone be classified as a "wire communication," and court was not free to hold otherwise. 18 U.S.C.A. § 2510(1, 2).

7. Criminal Law ⇨394.6(5)

Whether defendants had reasonable expectation that oral communications were not subject to interception was issue of fact to be determined on motion to suppress use of radio-telephone conversations. 18 U.S.C.A. § 2511(2)(b); Communications Act of 1934, § 3(a, b) as amended 47 U.S.C.A. § 153(a, b).

8. Searches and Seizures ⇨7(1)

Fourth Amendment offers protection for unreasonable searches but shuns absurd results. U.S.C.A.Const. Amend. 4.

9. Searches and Seizures ⇨7(1)

Not every electronic surveillance is constitutionally proscribed, and whether suppression is required must turn upon facts of case. U.S.C.A.Const. Amend. 4.

10. Searches and Seizures ⇨7(10)

If speaker has justifiable expectation that his conversation is subject to interception, speaker has not justifiably

relied on his privacy and Fourth Amendment is no impediment to interception, and whether there was justifiable reliance is factual question to be determined on motion to suppress use of radio-telephone conversations.

11. Telecommunications ⇨495

Party may not protest interception of oral communication if he was not participant in specific conversation. U.S.C.A.Const. Amend. 4.

John J. Flynn (argued), Thomas A. Thinner, Richard L. Parrish of Flynn, Kimerer, Thinner & Galbraith, Phoenix, Ariz., for appellant Dever.

Benjamin Lazarow, (argued), Tucson, Ariz., for appellants Hall and Nichols.

David S. Hoffman, Asst. U. S. Atty., (argued), William C. Smitherman, U. S. Atty., James M. Wilkes, Asst. U. S. Atty., Tucson, Ariz., for plaintiff-appellee.

Before WRIGHT and WALLACE, Circuit Judges, and FERGUSON,* District Judge.

WALLACE, Circuit Judge:

[1] Hall, Nichols and Dever were convicted of possession of marijuana with intent to distribute in violation of 21 U.S.C. § 841(a)(1) and conspiracy to commit that offense in violation of 21 U.S.C. § 846. Appellants contend that the electronic surveillance of their radio-telephone conversations which led to their arrests violated the Communications Act of 1934 (particularly, 47 U.S.C. § 605), Title III of the Omnibus Crime Control and Safe Streets Act of 1968,¹ and the Fourth Amendment. Therefore, they assert that the use of the conversations should have been suppressed. The district court was unpersuaded. We reverse.

Hall had radio-telephones installed in two automobiles. In early April, 1971, a Tucson housewife, who listens to her ra-

* Honorable Warren J. Ferguson, United States District Judge, Central District of California, sitting by designation.

1. Act of June 19, 1968, Pub.L.No. 90-351, § 802, 82 Stat. 212.

UNITED STATES v. HALL

Cite as 488 F.2d 193 (1973)

195

dio while doing housework, intercepted the appellants' conversations on her eight-band, 150-170 megacycle radio. The radio is not unique. The public may purchase similar sets on the open market and can listen to police and fire broadcasts, calls placed over the telephone companies' mobile telephone network; etc. After eavesdropping for less than a month, she reported what she considered to be suspicious conversations to the Arizona Department of Public Safety (DPS).

She continued to monitor the conversations and made reports to the DPS until at least May 21 when the DPS began its surveillance. Assuming that the period from the end of April until the 21st of May is not attributed to the DPS, there was still a five-week span until the appellants' arrests on July 2 during which the DPS conducted warrantless electronic surveillance of their conversations which led to their arrests.

[2] The arrests and convictions are inextricably bound to that warrantless search and seizure of their conversations.² That the state officers made the searches and arrests and then turned the case over to federal authorities for prosecution does not prevent the question from being raised. *Benanti v. United States*, 355 U.S. 96, 100, 78 S.Ct. 155, 2 L.Ed.2d 126 (1957). Therefore, affirmance of their convictions depends upon a determination of the validity of these searches.

I. Section 605.

[3,4] With certain exceptions not pertinent here, 47 U.S.C. § 605 forbids any person to intercept and divulge wire

2. The use of electronic devices to overhear a conversation is a search under the Fourth Amendment. *Berger v. New York*, 388 U.S. 41, 51, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967).

3. Act of June 19, 1968, Pub.L. No. 90-351, § 803, 82 Stat. 223. The amendment added the words "Except as authorized by chapter 119, title 18," to the beginning of § 605. Chapter 119 governs the procedure by which law enforcement personnel may secure a

or radio communications. In *United States v. Sugden*, 226 F.2d 281, 285 (9th Cir. 1955), *aff'd per curiam*, 351 U.S. 916, 76 S.Ct. 709, 100 L.Ed. 1449 (1956), we held "that unless the Congress orders otherwise" the exclusionary rule applies when non-FCC governmental agents or private individuals intercept non-public broadcasts without consent in violation of § 605. The first question before us is whether Congress has ordered otherwise.

Although only a few words were added to § 605 by the Crime Control Act,³ the legislative history of the Act clearly states that the amended section "is not intended merely to be a reenactment of section 605. The new provision is intended as a substitute." S.Rep.No.1097, 90th Cong., 2d Sess., 1968 U.S.Code Cong. and Admin.News 2196. The legislative history also explicitly shows that Congress intended to exclude law enforcement officers from the purview of the new § 605. The Senate Judiciary Committee stated:

The new section is designed to regulate the conduct of communications personnel. It also provides that no person not authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person. "*Person*" does not include a law enforcement officer acting in the normal course of his duties. But see *United States v. Sugden* (226 F.2d 281 (9th Cir. 1955)), *affirmed per curiam*, 76 S.Ct. 709, 351 U.S. 916 [100 L.Ed. 1449] (1956).

warrant for electronic surveillance. The government argues that this amends the section in two ways. First, that it incorporates a requirement of expectation of privacy and second, that it changes the protection of the section from the means of conversation to the conversation itself. See *Goldman v. United States*, 316 U.S. 129, 133, 62 S.Ct. 993, 86 L. Ed. 1322 (1942); *Sugden, supra*, 226 F.2d at 284. We need not reach these questions because we hold § 605 does not apply to the facts of this case.

Id. at 2197 (emphasis added to text). It is obvious that the legislature wanted law enforcement personnel to be governed exclusively by Chapter 119 of Title 18. Therefore, because the critical communications were intercepted by the lawmen, § 605 offers no impediment. We need not reach the question of the involvement of the housewife.⁴

II. Chapter 119 of Title 18.

[5, 6] Whether the challenged interception should be suppressed demands close scrutiny of the statutory requirements concerning wire and oral communications added by Title III of the Crime Control Act. See Chapter 119, 18 U.S.C. § 2510 et seq. If the interception in question falls within the parameters of Chapter 119, the warrantless surveillance must be suppressed. 18 U.S.C. § 2515.

The threshold question is whether these radio-telephone conversations constitute an "oral communication" or a "wire communication." The answer is critical because the definition of oral communication includes the expectation of privacy language derived from *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). In order for an oral communication to be protected by the Act, the speaker must have "an expectation that such communication is not subject to interception under circumstances justifying such expectation" 18 U.S.C. § 2510(2). A "wire communication" has no such restriction in its definition. It is defined as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception . . ." 18 U.S.C. § 2510(1).

4. We note that § 605 forbids divulgence of restricted communications to "any person." As a law enforcement officer is not a "person" under § 605, it is questionable whether the communications by the housewife to the DPS would be in violation of this section.

Obviously, there is a reason for the more restrictive definition of oral communications. When a person talks by telephone, he can reasonably assume privacy. That assumption may often be invalid for non-wire communications. Therefore, it is incumbent upon the participants in an oral communication to make a reasonable estimate of the privacy afforded them by their particular circumstances.

The definition of wire communication is not free from ambiguity. "[C]ommunication made in whole or in part . . . through the use of facilities . . . by the aid of wire . . . between the point of origin and the point of reception . . ." could be interpreted in several ways. For example, it could be argued that if any wire is used to aid the communication, it must be deemed a wire communication. If this were followed to its conclusion, the use of a radio would be included in the definition because some wires are contained in the radio transmitter and receiver—thus the communication would be aided "in part" by the use of wire. However, such an interpretation would be inconsistent with the language of the immediately succeeding section which permits an agent of the FCC, in certain circumstances, "to intercept a wire communication, or oral communication transmitted by radio . . ." 18 U.S.C. § 2511(2)(b).⁵

Broadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire. As with any broadcast into the air, the invitation to listen is afforded to all those who can hear. In the instant case, the eavesdroppers merely tuned their radio receivers to the proper station. It is obvious that conversations initiated from a

5. It would also be inconsistent with the mutually exclusive definitions of "wire" and "radio" communications found in the Communications Act of 1934. 47 U.S.C. § 153(a) & (b).

UNITED STATES v. HALL

197

CITE AS 488 F.2d 193 (1973)

radio-telephone more logically fall within the category of "oral communication."

By reading the sections together, we can only conclude that the Congress did not mean that every conversation aided in any part by any wire would be a wire communication. As a radio broadcast must be deemed an oral conversation, we believe it would strain the legislative intent to hold that conversations emanating from a radio telephone would not be treated similarly.

However, that does not end our inquiry. Although the record is not clear, it appears that some conversations were between two radio telephones while others were between a radio telephone and a regular land-line telephone. While the former are within the definition of oral communications, the use of a land-line telephone at one end of the conversation raises a serious question as to the defined category in which such a communication belongs. While logic may dictate that the same rule should apply when a conversation crosses the airways but initiates or terminates on a land line, we are not free to reach that result if the legislative intent is to the contrary.

The legislative history states:

Paragraph (1) defines "wire communication" to include all communications carried by a common carrier, in whole or in part, through our Nation's communications network. The coverage is intended to be comprehensive.

6. See 18 U.S.C. §§ 2511, 2520.

7. See, e.g., S.Rep.No.1097, 90th Cong., 2d Sess., 1968 U.S.Code Cong. and Admin.News 2112; Hearings on Controlling Crime through More Effective Law Enforcement Before the Subcomm. on Criminal Laws and Procedure of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess. (1967); Hearings on the Right of Privacy Act of 1967 Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary, 90th Cong., 1st Sess. (1967); Hearings on Criminal Laws and Procedure Before the Subcomm. on Criminal Laws and Procedure of the Senate Comm. on the Judiciary, 89th Cong., 2d Sess. (1966).

G. Robert Blakey, now a staff member of the Senate Criminal Laws and Procedure

S.Rep.No.1097, 90th Cong., 2d Sess., 1968 U.S.Code Cong. and Admin.News 2178. Based upon this indication of Congressional intent, we are forced to conclude that, when part of a communication is carried to or from a land-line telephone, the entire conversation is a wire communication and a search warrant is required.

We realize that our classification of a conversation between a mobile and a land-line telephone as a wire communication produces what appears to be an absurd result. These conversations were intercepted by an ordinary radio receiver and not by a phone tap. Logically they should be afforded no more protection than those occurring between two radio transceivers. They should be oral communications. However, Congress's definition of a wire communication necessitates this conclusion.

This is especially ironic since Title III of the Crime Control Act contains stringent civil and criminal penalties for those who violate its provisions.⁶ In other words, any citizen who listens to a mobile telephone band does so at its own risk, and scores of mariners who listen to the ship-to-shore frequency, commonly used to call to a land-line telephone, commit criminal acts.

However we have closely examined the legislative history of Title III and have found no indication of how Congress intended to treat a radio-telephone conversation.⁷ In the absence of such

Subcommittee, is the acknowledged author of Title III and other related works on eavesdropping. Schwartz, *The Legitimation of Electronic Eavesdropping: The Politics of Law and Order*, 67 Mich.L.Rev. 454, 456-57 & n. 10 (1969). We also have studied his writings and have found no solution. See, e.g., American Bar Association Project on Minimum Standards for Criminal Justice: Standards Relating to Electronic Surveillance (Approved Draft 1971); President's Commission on Law Enforcement and the Administration of Justice, *Task Force Report: Organized Crime* 80, 91-113 (1967); Blakey & Hancock, *A Proposed Electronic Surveillance Control Act*, 43 Notre Dame Law. 657 (1968).

an indication, we must conclude that, if the conversation involves a land-line telephone, it is a wire communication.

We have the option to use the "surely Congress did not intend" rubric and amend the statute. But usurpation of the legislative function by the courts is a basic violation of the separation of powers doctrine. We reject that alternative. Any change must therefore be made by the Congress.

[7] The trial court should now determine whether the arrests resulted from interceptions of oral or wire communications. If from wire communications, the warrantless interception should be suppressed as to those with standing to object. If not from wire communications, the critical question then becomes whether appellants had a reasonable expectation that the communications were not subject to interception. This too is an issue of fact to be determined by the trial court at the time of the motion to suppress. The district judge made a specific finding that Hall and Nichols knew they could be heard by other people and had no right of privacy. The record substantiates this finding and it is not clearly erroneous. *United States v. Gunn*, 428 F.2d 1057, 1060 (5th Cir. 1970); 3 C. Wright, *Federal Practice and Procedure* § 675, at 130 (1969). The judge stated he could not, from the evidence, make such a finding as to Dever.

Therefore, as to any conversations not involving a land-line telephone by Hall and Nichols, the interceptions were not "oral communications" as defined because they lacked the requisite expectation of privacy. Thus, no search warrant was required by the statute. As to Dever, the result may be different.

III. *The Fourth Amendment.*

[8,9] But interceptions not within the statutory definition of oral or wire communications still must meet the test of the Fourth Amendment. Electronic surveillance has come under close scrutiny by the courts and properly so. The

ingenious mind of man can conjure up subtle methods of search through modern electronics as reprehensible as kicking down a door. While the Fourth Amendment offers protection from searches when unreasonable, it shuns absurd results. Every electronic surveillance is not constitutionally proscribed and whether the interception is to be suppressed must turn upon the facts of each case.

It would be absurd to hold that one is constitutionally protected from any untoward results when he makes statements at a time when he has reason to know some third party is, or probably is, listening. We have, therefore, held that "for suppression of overheard speech the speaker must have 'justifiably relied' on his privacy." *United States v. Fisch*, 474 F.2d 1071, 1076 (9th Cir. 1973) (footnote omitted); see *Katz, supra*, 389 U.S. at 351-353, 88 S.Ct. at 511-512. In interpreting the justifiable reliance language of *Katz*, we have leaned heavily on Mr. Justice Harlan's analysis:

As the concurring opinion of Mr. Justice Harlan makes clear, the concept of justifiable reliance involves both subjective and objective aspects. There must, first of all, have been a reliance on, an actual and reasonable expectation of, privacy. But beyond the individual's expectations, the needs of society are involved. The individual's subjective, self-centered expectation of privacy is not enough. We live in an organized society and the individual's expectation of privacy must be justifiable, "one that society is prepared to recognize as 'reasonable.'"

Fisch, supra, 474 F.2d at 1076-1077 (footnote omitted).

[10] Whether there was justifiable reliance is a factual question to be determined by the trial court. We discern no difference in substance between the test under the Fourth Amendment and that involved in the definition of oral communications under 18 U.S.C. § 2510(2). Thus, if a speaker has a justifi-

UNITED STATES v. HALL

CITE AS 488 F.2d 193 (1973)

199

fiable expectation that his conversation is subject to interception and therefore it is not an "oral communication," then the speaker has not justifiably relied on his privacy and the Fourth Amendment is no impediment to interception.

IV. Conclusion.

[11] The record is unclear as to whether the critical conversations were oral or wire communications. The case must be remanded for findings on this issue consistent with our opinion. Furthermore after the district court determines that question, if it finds that the communications were oral, then it must decide if the parties had a reasonable expectation of privacy. It has already determined that Hall and Nichols did not. Finally after these conclusions, the court must insure that the objecting party has standing to complain of the interception. See *Jones v. United States*, 362 U.S. 257, 261, 80 S.Ct. 725, 4 L.Ed.2d 697 (1960). If the intercepted communications were oral, and if either Hall or Nichols were parties, then they cannot complain because they did not expect privacy. In addition, a party may not protest if he was not a participant in a specific conversation.

Reversed and remanded.

FERGUSON, District Judge (dissenting in part):

I respectfully dissent from Part I of the court's decision. In my view, 47 U.S.C. § 605 requires a reversal of the convictions.

Section 605 provides in pertinent part:

"Except as authorized by chapter 119, Title 18, no person receiving any interstate communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except [in certain situations not here applicable]. No person not being authorized by the sender shall intercept any radio communication and divulge or publish the

existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person.

It is clear that prior to the 1968 amendment, the word "person" in § 605 encompassed law enforcement officials. *Lee v. Florida*, 392 U.S. 378, 88 S.Ct. 2096, 20 L.Ed.2d 1166 (1968); *Nardone v. United States*, 302 U.S. 379, 58 S.Ct. 275, 82 L.Ed. 314 (1937). In *Lee*, the Supreme Court squarely faced the issue:

"In [*Nardone*], the Court was first called upon to decide whether § 605 had indeed served to render evidence of intercepted communications inadmissible in a federal trial. In that case the Government urged that 'a construction be given the section which would exclude federal agents since it is improbable Congress intended to hamper and impede the activities of the government in the detection and punishment of crime.' 302 U.S., at 383 [58 S.Ct. at 277]. In reversing the judgment of conviction, the Court's answer to that argument was unequivocal:

'[T]he plain words of § 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that "no person" shall divulge or publish the message or its substance to "any person." To recite the contents of the message in testimony before a court is to divulge the message. The conclusion that the act forbids such testimony seems to us unshaken by the government's arguments.

* * * * *

'Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty. The same considerations may well have moved the Congress to adopt § 605 as evoked the guaranty against practices and proce-

dures violative of privacy, embodied in the Fourth and Fifth Amendments of the Constitution.' 302 U.S., at 382, 383 [58 S.Ct. at 276]." 392 U.S. at 382-383, 88 S.Ct. at 2099-2100.

Section 605 as amended in 1968 likewise provides that "no person" shall divulge any communication covered by the statute to "any person." The statutory language is clear and unambiguous. Nowhere in the statute is the word "person" restricted, limited, or modified. If the words of the statute are interpreted according to their plain meaning, § 605 clearly applies to law enforcement officers.

The majority fastens on two sentences in the Senate report to the Omnibus Crime Control and Safe Streets Act of 1968 to support its conclusion that § 605 as amended does not apply to law enforcement officials:

"'Person' does not include a law enforcement officer acting in the normal course of his duties. But see *United States v. Sugden* (226 F.2d 281 (9th Cir. 1955), *affirmed per curiam*, 76 S.Ct. 709, 351 U.S. 916 [100 L.Ed. 1449] (1956))." S.Rep.No.1097, 90th Cong., 2d Sess., 1968 U.S.Code Cong. & Admin.News, pp. 2112, 2197.

The reference to the *Sugden* case was clearly intended to emphasize the word "normal" in the preceding sentence. In *Sugden*, short wave radio transmissions on a private farm were monitored by a Federal Communications Commission employee and were then used to prosecute the broadcasters for immigration law violations. This court, by Judge Chambers, noted that the "theory of conduct" of the immigration officers "seems to have been, 'The Federal Communications Commission can legally listen. So we shall use their ears for what we, the Immigration Service, cannot do.'" 226 F.2d at 285. The court held that the intercepted conversations were inadmissible as long as the radio station was legally on the air and the operators were legally authorized to operate it.

The majority's conclusion in Part I that § 605 does not compel a reversal of the convictions in these cases turns on the statement in the Senate report that "'Person' does not include a law enforcement officer acting in the normal course of his duties." I would hold that where, as here, the statutory language is clear and unambiguous, and where Congress could easily have incorporated any intended restriction or limitation on the meaning of any word in the statute itself, the words of the statute must be interpreted according to their plain meaning, and the statutory language must control.

It is a well-established principle of law that "there is no need to refer to the legislative history where the statutory language is clear." *Ex parte Collett*, 337 U.S. 55, 61, 69 S.Ct. 944-947, 93 L. Ed. 1207 (1949). In *Eason v. Commissioner of Internal Revenue*, 294 F.2d 653, 656 (9th Cir. 1961), this court held that "[w]hen a statute is unambiguous, the courts may not look elsewhere for the legislative intent." In *United States v. Oregon*, 366 U.S. 643, 648, 81 S.Ct. 1278, 1281, 6 L.Ed.2d 575 (1961), the Supreme Court stated, "Having concluded that the provisions of § 1 [of the statute in question] are clear and unequivocal on their face, we find no need to resort to the legislative history of the Act." (Footnote omitted.) This principle of statutory interpretation has been applied in many cases. *See Ex parte Collett, supra*, 337 U.S. at 58; 69 S.Ct. 944; *Arkansas Valley Industries, Inc. v. Freeman*, 415 F.2d 713, 717 (8th Cir. 1969); *Sea-Land Service, Inc. v. Federal Maritime Commission*, 404 F.2d 824, 828 (D.C. Cir. 1968); *Department Employees' Local 1265 v. Brown*, 284 F.2d 619, 627 (9th Cir.), cert. denied, 366 U.S. 934, 81 S.Ct. 1659, 6 L.Ed.2d 846 (1961).

The principle that clear and unambiguous statutory language must prevail over a conflicting statement in the legislative history holds true particularly where, as here, the same language was contained and authoritatively construed

UNITED STATES v. HALL

201

Cite as 488 F.2d 193 (1973)

in an earlier version of the statute. If Congress had intended to restrict or limit the meaning of the word "person" in the 1968 amendment, it could easily have done so in the statute itself. Indeed, Congress did explicitly distinguish between "person" and "law enforcement officer" in another section of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510, enacted (with 47 U.S.C. § 605) in Title III of the Act, contains separate definitions for "person" and for "Investigative and law enforcement officer." These definitions apply to the provisions of chapter 119 of Title 18, 18 U.S.C. §§ 2510-20. If Congress had intended law enforcement officers to be excluded from the word "person" in § 605, it manifestly would have done so through clear statutory language, as it did in 18 U.S.C. § 2510.

The majority also seeks support for its conclusion in Part I in the statement in the Senate report that the amended section "is not intended merely to be a reenactment of section 605. The new provision is intended as a substitute." 1968 U.S.Code Cong. & Admin.News, at p. 2196. In my view, this statement was intended to emphasize that the scope of coverage of § 605 was narrowed by the 1968 amendment, and that part of the area formerly regulated by § 605 was now to be regulated by chapter 119 of Title 18, 18 U.S.C. §§ 2510-20. Whereas formerly the provisions of § 605 applied to both wire and radio communications, the amendment restricted the scope of all provisions after the first sentence to radio communications. The amendment

inserted the word "radio" before "communication" in the second and fourth sentences, deleted the phrase "wire or" preceding "radio" in the third sentence, and added the introductory clause "Except as authorized by chapter 119, Title 18," 47 U.S.C. § 605. In these respects, the amended section was a "substitute" for, and not merely a "reenactment of," § 605.

One court has held that § 605 as amended renders evidence of telephonic communications intercepted by police officers inadmissible. In *People v. Trief*, 65 Misc.2d 272, 317 N.Y.S.2d 525 (1970), *aff'd mem.*, 37 A.D.2d 553, 323 N.Y.S.2d 659 (1971), the prosecution sought to introduce evidence obtained from telephone conversations intercepted by police officers. The prosecution conceded that prior to the 1968 amendment, the intercepted conversations would have been inadmissible, but contended that the amendment rendered them admissible. The court squarely rejected this view, holding that under § 605 as amended, the intercepted conversations must be suppressed.¹ *Cf. Commonwealth v. Coviello*, Mass., 291 N.E.2d 416 (1973).

The government concedes that the convictions of the defendants were possible only because of the intercepted communications. I would hold that the divulgence of those communications to the officers of the Arizona Department of Public Safety and their divulgence by the officers at trial violated 47 U.S.C. § 605, and I would reverse the convictions.²

1. While *People v. Trief* involved interceptions of wire rather than oral communications, its interpretation of § 605 to prohibit the divulgence of conversations intercepted by police officers does not depend upon the distinction between oral and wire communications. If § 605 applies to law enforcement officials, it covers interceptions of oral as well as wire communications.

2. It is clear that no expectation-of-privacy requirement is contained in § 605. *United States v. Sugden*, *supra*, 226 F.2d at 284-285; *United States v. Laughlin*, 226 F.Supp. 112 (D.D.C.1964); *United States v. Fuller*, 202 F.Supp. 356 (N.D.Cal.1962).

under some circumstances failure of retained counsel to prosecute an appeal can be such as to deprive an accused of his constitutional rights to counsel. This was said to be especially true if retained counsel abandoned the appeal without accused's consent or without any warning so as to deprive him of his right of appeal. *Woodall v. Neil*, supra, at 93. Any such uncommunicated withdrawal of counsel from the case immediately after trial constitutes a denial of the right to an appeal.

[2] Here, the state district court held a plenary hearing on this petition and expressly found that employed counsel had failed, not only to prosecute any appeal from petitioner's conviction, but also to advise him that no appeal would be taken on his behalf. In view of *Chapman*, petitioner's complaint may be meritorious. However, that determination should be left up to the state forum. State courts should be given the first opportunity to pass upon and correct errors of federal law in a state prisoner's conviction. It must not be assumed that state courts will be derelict in their duty to give full effect to federal constitutional rights, when warranted.

This tenet complements the doctrine of abstention, whereby full play is allowed the states in the administration of their criminal justice. To allow the state judiciary the initial inquiry is a matter of accommodation between state and federal courts. This concept is grounded primarily upon respect which federal courts should and do have for state judicial processes. *Younger v. Harris*, 401 U.S. 37, 91 S.Ct. 746, 27 L. Ed.2d 669 (1970). It is not one defining power but one which relates to the appropriate exercise of power. *Fay v. Noia*, 372 U.S. 391, 83 S.Ct. 822, 9 L. Ed.2d 837 (1967). Every consideration of comity and propriety demands that in cases of this character, recourse should first be had in the state courts.

[3] Therefore, the proper action for this Court is to defer any decision at this time until the Court of Criminal

Appeals, which is already cognizant of the litigation, has the occasion to review the issue. A practical appraisal of the state interest involved here plainly justifies the federal court's staying its hand, thereby giving finality to state judicial procedures.

Now, therefore, it is ordered, adjudged and decreed that petitioner has thirty (30) days from this date in which to present his petition to the Court of Criminal Appeals of Texas. Should he fail to do so, the petition will be dismissed.



Rufus Lee SMITH, Plaintiff,
v.
Howard R. WUNKER, Defendant.
No. 8081.

United States District Court,
S. D. Ohio, W. D.
April 13, 1972.

Civil action by one party to telephone conversation against other party for alleged wrongful recording and disclosure of conversation without knowledge or consent of the plaintiff. On motion to dismiss, the District Court, Porter, J., held that the recording of private telephone conversation by a party to it and its subsequent disclosure did not violate statutes making it unlawful to intercept wire or oral communication.

Motion granted and complaint dismissed with prejudice.

1. Statutes \Rightarrow 184

In construing statute, court would look to the act itself and legislative purpose behind it.

2. Telecommunications \Rightarrow 492

Purpose of act pertaining to wire interception and interception of oral

communications was to prohibit any unauthorized interception of wire or oral communications and use of the contents thereof in evidence in courts and administrative proceedings and to safeguard the privacy of innocent persons from interception, where none of the parties consented to the interception. 18 U.S.C.A. §§ 2510(4), 2510 note, 2511(2)(d).

3. Telecommunications ⇨494

"Aural acquisition" within criminal statute which defines "intercept" for purposes of statutes prohibiting unauthorized interception of wire or oral communications means to come into possession through the sense of hearing. 18 U.S.C.A. §§ 2510(4), 2510 note, 2511(2)(d).

See publication Words and Phrases for other judicial constructions and definitions.

4. Telecommunications ⇨495

The recording of private telephone conversation by a party to it and its subsequent disclosure did not violate statutes making it unlawful to intercept wire or oral communication. 18 U.S.C.A. §§ 2510(5), (5)(a), 2511(2)(d), 2515.

5. Telecommunications ⇨495

One who is party to telephone conversation may repeat it verbatim without the use of recording device and not violate statutes prohibiting wire interception and interception of oral communications. 18 U.S.C.A. §§ 2510(5), (5)(a), 2511(2)(d), 2515.

6. Telecommunications ⇨495

One who was party to telephone conversation was not "eavesdropping" or "wiretapping" when he recorded such conversation. 18 U.S.C.A. §§ 2510(5), (5)(a), 2511(2)(d), 2515.

See publication Words and Phrases for other judicial constructions and definitions.

Harvey B. Woods, Cincinnati, Ohio,
for plaintiff.

Richard C. Curry, Cincinnati, Ohio,
for defendant.

OPINION AND ORDER

PORTER, District Judge.

In this case there is a motion to dismiss submitted for decision. This requires a determination of whether a party to a phone conversation may record it and disclose it without violating 18 U.S.C. § 2510 et seq. (wire interception and interception of oral communications).

The defendant's motion to dismiss was filed pursuant to Rule 12(b) F.R.Civ.P. on the grounds that the complaint failed to state a cause of action. The motion is unopposed. Under Local Rule 14, failure to file a memorandum *contra* may be cause for the Court to grant the motion as filed. Though the failure to file a memo by plaintiff's counsel is inexcusable and reason enough for a censure, the motion is considered on its merits.

"For purposes of the motion to dismiss the complaint is construed in the light most favorable to plaintiff and its allegations are taken as true. The court's inquiry is directed to whether the allegations constitute a statement of a claim under Rule 8(a)." Wright & Miller, *Federal Practice and Procedure*, Vol. 5, p. 594.

The pertinent allegations of the complaint are as follows:

"Plaintiff states that in July of 1969, defendant recorded and disclosed an alleged telephone conversation between plaintiff and defendant without the knowledge or consent of the plaintiff.

"Defendant disclosed said alleged conversation to employees and agents of The Cincinnati Post & Times-Star, said alleged conversation or excerpts therefrom being printed in said publication.

"That newspaper reports of said conversation purport to be an attempt by the plaintiff to obtain money from defendant for intervening in and 'fixing' a matter pending in the Common Pleas Court, Hamilton County, Ohio."

In other paragraphs of the complaint there are allegations that there was a willful disclosure of the conversation to the general public through a newspaper and the interception, as well as the disclosure, was willful.

[1] We have not been cited to any case in point, nor have we found one. We therefore look to the Act itself and the legislative purpose behind it.

[2] Such purpose was to prohibit any unauthorized interception of wire or oral communications and the use of the contents thereof in evidence in courts and administrative proceedings. (Pub. L. 90-351 § 801(b), 18 U.S.C. § 2510 nt.) This part of the Act was also concerned with safeguarding the privacy of innocent persons from interception, where none of the parties consented to the interception. (Pub. L. 90-351 § 801(d), 18 U.S.C. § 2510 nt.)

Since the complaint shows that the defendant was not acting under color of law the pertinent section of the Act is 18 U.S.C. § 2511(2)(d). That provides:

"It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State or for the purpose of committing any other injurious act."

Under this we must determine whether there has been an "interception." That term is defined in the statute as follows:

"(4) 'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. § 2510(4).

"Electronic, mechanical, or other device" is defined in 18 U.S.C. § 2510(5) and means:

" . . . any device or apparatus which can be used to intercept a wire or oral communication other than—

"(a) any telephone . . . (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; * * *"

[3] The words "aural acquisition" literally translated mean to come into possession through the sense of hearing (Webster's Third New International Dictionary, 1967 Ed.).

[4] We conclude the recording of a private conversation by a party to it and its subsequent disclosure does not violate 18 U.S.C. § 2511(2)(d) or any other section in the chapter beginning with § 2510, 18 U.S.C., entitled "Wire Interception and Interception of Oral Communications."

[5] This is borne out by the congressional findings stated in § 801 of Public Law 90-351, 18 U.S.C. § 2510 nt. The findings show a concern with devices that "overhear" conversations and not devices that record conversations. The means of "aural acquisition" in this case is the telephone itself, and, of course, that is clearly exempted by 18 U.S.C. § 2510(5)(a). We note that the defendant as a party to the conversation could have repeated it verbatim without the use of a recording device and that would not come within the purview of 18 U.S.C. § 2515.

As far as the legislative history is concerned, we find, at page 2154 U.S. Code, Cong. & Admin. News of 1968, the concern of Congress was with the interception of private conversations by an unseen auditor and turning such intercepted conversation against the speaker to the auditor's advantage.

It was there indicated, at page 2182, that 18 U.S.C. § 2511(2)(d), which grants an exemption to parties to the conversation, largely reflects existing law, citing *Rathbun v. United States*, 355 U.S. 107, 78 S.Ct. 161, 2 L.Ed.2d 134

MAES v. MOTIVATION FOR TOMORROW, INC.

47

Cite as 356 F.Supp. 47 (1973)

(1957) and *Lopez v. United States*, 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963). In *Rathbun* the contents of a conversation overheard on a regularly used telephone extension, with the consent of one of the parties to the conversation, was found to be admissible in federal court. The Court stated at 355 U.S. at page 110, 78 S.Ct. at page 163:

"The clear inference is that one entitled to receive the communication may use it for his own behalf or have another use it for him. The communication itself is not privileged, one party may not force the other to secrecy merely by using a telephone."

Lopez strikes us as very much like the instant case. There a Federal Revenue Agent used a pocket wire recorder to record a conversation that he had with the defendant. The Court permitted the recording to be introduced in evidence against the defendant, stating that the recording of a conversation by one privileged to hear it is not eavesdropping in any proper sense of the word. The Court said, 373 U.S. at page 440, 83 S.Ct. at page 1389:

"Indeed, there has not even been any electronic eavesdropping on a private conversation which government agents could not have otherwise overheard."

[6] By the same token, the defendant herein who was a party to the conversation was not "eavesdropping" or "wiretapping" when he recorded such conversation.

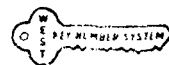
Finally, we note that the Administration, speaking through its Attorney General, criticized the proposed legislation because it exempted all consensual wiretapping and eavesdropping. The statement of the Attorney General was as follows:

"Thus, although the title contains blanket prohibitions on all 'third-party' ('nonconsensual') interceptions—that is, interceptions without the consent of at least one of the parties to a conversation—by private persons, and places strict control on the use of such interceptions by law enforcement offi-

cers, it is totally permissive with respect to surreptitious monitoring of a conversation by a party to the conversation, even though the monitoring may be for insidious purposes such as blackmail, stealing business secrets, or other criminal or tortious acts in violation of Federal or State laws."

The Attorney General included the recording of a conversation by a party to it as an act allowed under the Act.

To recapitulate, we find the motion is well taken. It is obvious that the complaint cannot be amended to state a cause of action. It is therefore ordered that the complaint be dismissed with prejudice.



Rudolph J. MAES and Leola Maes, on behalf of themselves and all other persons similarly situated, Plaintiffs,

v.

MOTIVATION FOR TOMORROW, INC., a corporation, Webster Home Plan Inc., a corporation, etc., Defendants.

No. 72968.

United States District Court,
N. D. California.

March 7, 1973.

Buyers brought action under Consumer Credit Protection Plan seeking damages from seller and its associate for alleged failure to comply with disclosure requirements under the Act for sales not under open end credit plans. On defendants' motions to dismiss or, in the alternative, for summary judgment, the District Court, Sweigert, J., held that complaint which attached agreement in question containing statement that "Additional Products or Services may be purchased by the buyer from time to time and added to the balance of this Open Account within credit limits

No. 80-1391

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

ABDEEN M. JABARA,

Plaintiff-Appellee,

v.

WILLIAM H. WEBSTER, ET AL.,

Defendants-Appellants.

ON APPEAL from the
United States District
Court for the Eastern
District of Michigan,
Southern Division.

Decided and Filed October 21, 1982

Before: MARTIN, Circuit Judge; PECK and BROWN,* Senior Circuit Judges.

BAILEY BROWN, J. Appellee, Abdeen M. Jabara (Jabara), a Detroit lawyer of Arab extraction, has over the years been interested and active in Arab causes. The Federal Bureau of Investigation (FBI), as a result of his activities, began an investigation of him in 1967. This investigation was not continuous and varied from time to time as to intensity and as to the technique used. The technique used by the FBI included physical surveillance by agents and informants, including his speech-making activities, inspection of Jabara's bank records, warrantless electronic surveillance by the National Security Agency (NSA), and interviews of third parties regarding Jabara. This information was maintained and disseminated by the FBI.

* Circuit Judge Brown retired from regular active service under the provisions of 28 U.S.C. § 371(b) on June 18, 1982, and became a Senior Circuit Judge.

Jabara filed an action in district court in Detroit in October, 1972, alleging several causes of action. The defendants include the Attorney General, the Directors of the FBI and NSA in their official capacities and certain known and unknown officers and employees of the FBI and the NSA. One cause of action alleged was that Jabara's fourth amendment rights were violated as a result of NSA's interception of his "communications by means of warrantless electronic surveillance and/or disclosed summaries of these interceptions to the Federal Bureau of Investigation."¹ Another cause of action alleged was that the defendants violated a provision of the Privacy Act, 5 U.S.C. § 552a(e)(7), by maintaining records with respect to Jabara's exercise of his first amendment rights. The district judge, on cross-motions for summary judgment, granted judgment and injunctive relief to Jabara as to both of these claims and defendants appealed.²

I.

A preliminary question presented on this appeal is whether this court can, as contended by defendants, properly consider *in camera* the classified appendix that defendants filed in the district court.³ Jabara's position is that this court should not consider the materials in the classified appendix at all unless the materials are made available to him or at least to his counsel subject to a protective order. The district court determined (75 F.R.D. 475, 487 (1977)) that these materials, because they are properly protected by the state secret privilege, should be submitted *in camera*; this was done without

¹ Second amended complaint. (App. at 69).

² The history of this litigation, including citations to reported opinions dealing with resolution of discovery issues, is clearly and fully set out in the opinion of the district court resulting in the grant of summary judgment and injunctive relief. *Jabara v. Kelley*, 476 F. Supp. 561 (E.D. Mich. 1979).

³ *In camera* treatment and the assertion of the state secret privilege were supported by the *in camera* affidavits of Defendants Schlesinger, Rumsfeld and Brown.

access by Jabara or his counsel. We conclude that the district court was correct in its ruling and, further, that this court likewise may properly receive *in camera* and so consider such materials in the classified appendix. *United States v. Reynolds*, 345 U.S. 1 (1953); *Kerr v. United States District Court for the Northern District of California*, 428 U.S. 394 (1976); and *Halkin v. Helms*, 598 F.2d 1 (D.C. Cir. 1978). || *

II.

To understand the fourth amendment issue raised by the NSA's interception of Jabara's communications and supplying these to the FBI, all without a warrant, it is necessary briefly to describe the factual background of this claim and then to outline the contentions of the parties.

The NSA intelligence gathering operation is described sufficiently for present purposes in *Halkin*, 598 F.2d at 4. as follows (footnote omitted):⁴

A brief description of NSA and its functions is appropriate. NSA itself has no need for intelligence information; rather, it is a service organization which produces intelligence in response to the requirements of the Director of Central Intelligence. Intelligence Activities: Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the U.S. Senate, 94th Cong., 1st Sess. Vol. V at 9 (1975) (Hearings). The mission of the NSA is to obtain intelligence from foreign electrical communications. Signals are acquired by many techniques. The process sweeps up enormous numbers of communications, not all of which can be reviewed by intelligence analysts. Using "watch-lists"—lists of words and phrases designed to identify communications of intelligence interest—NSA computers scan the mass of acquired communications to select those which may be of specific foreign intelligence interest. || *

⁴ See also: Note, *Government Monitoring of International Electronics Communications: National Security Agency Watch List Surveillance and the Fourth Amendment*, 67 *U. Cal. L. Rev.* 689 (1978). || *

Only those likely to be of interest are printed out for further analysis, the remainder being discarded without reading or review. Intelligence analysts review each of the communications selected. The foreign intelligence derived from these signals is reported to the various agencies that have requested it (Hearings at 6). Only foreign communications are acquired, that is, communications having at least one foreign terminal (Hearings at 9).

On November 1, 1971, the FBI, without a warrant, requested the NSA to supply it with the contents of Jabara's telegraphic communications sent overseas, and the NSA complied by furnishing the FBI with summaries of six of such communications.

Defendants contend that the fourth amendment does not apply to and limit NSA's gathering of foreign intelligence. They also contend that, in any event, the facts surrounding the acquisition by the NSA of overseas telegraphic communications such as those sent by Jabara are subject to the state secret privilege.⁵

Jabara, however, does not even contend on this appeal that the interception by the NSA violated his fourth amendment rights; we may therefore take as a given that the information was legally in the hands of the NSA. What Jabara does contend, and the district court agreed, is that his rights were violated when the NSA turned over the information, without a warrant, to the FBI. Defendants, on the other hand, contend that, since the NSA had lawfully intercepted and had made a record of the content of Jabara's communications, the fourth amendment was not implicated when the FBI requested and obtained the summaries from the NSA. This is so, defendants contend, because there simply was no "search" or "seizure"

⁵ This was so held in *Halkin*, *supra*; indeed in *Halkin*, it was held that, pursuant to the state secret privilege, the government did not even have to divulge to plaintiffs whether the NSA had intercepted their overseas communications. Here, as previously indicated, the government has divulged in the open record that NSA did intercept and later turn over to the FBI Jabara's communications.

when this information was turned over to another agency of the government.

Defendants still further contend that, even if there was a "search" or "seizure" when the FBI obtained the summaries from the NSA, a warrant was not required because there is a "foreign agent" exception to the warrant requirement and the foreign agent exception was applicable here since, at the time the FBI made the request for the summaries, it had reasonable cause to believe that Jabara was in fact a foreign agent. Jabara, on the other hand, contends that there is no foreign agent exception to the warrant requirement and that, in any event, at the time the FBI made the request, it had no reasonable cause to believe that he was a foreign agent.

In connection with defendants' contention that the FBI had reasonable cause to believe that Jabara was a foreign agent when it requested the summaries, there is a threshold procedural issue. After the district court had made its decision that Jabara's fourth amendment rights were violated when the summaries were supplied to the FBI (476 F.Supp. 561 (1979)), defendants moved for reconsideration and filed additional open and *in camera* affidavits⁶ to support their contention that, at the time the FBI made the request for the summaries, it had reasonable cause to believe that Jabara was a foreign agent. The defendants argued, in support of their motion to reconsider, that they had been surprised by the court's decision that the FBI's acquisition of the summaries was a fourth amendment violation since they had thought that the controlling issue was the legality of the NSA's interception of the overseas telegraphic communications. Defendants further argued that, since the NSA's interception of the overseas

⁶ These affidavits were executed by Special Agent French of the FBI, who is in the Records Management Division in Washington. Defendants contend that these affidavits, particularly the *in camera* one, demonstrate that on the day the FBI requested the summaries of Jabara's overseas communications from NSA, November 1, 1971, it had received solid information from the Central Intelligence Agency that Jabara was, indeed, a senior member of a Middle East terrorist organization.

telegraphic communications in performance of its foreign intelligence function did not invade Jabara's fourth amendment rights whether or not Jabara was a foreign agent, they had no reason to emphasize the FBI's reasonable belief that he was. The district court, in its unreported memorandum denying the motion to reconsider (App. at 190), determined that the question whether there was cause to believe Jabara was a foreign agent had been an issue in the case and that it had theretofore determined (75 F.R.D. at 493) that, in the record then before it, there was no evidence that Jabara was connected with or was a foreign agent.⁷ The district court further determined that the additional affidavits executed by FBI agent French and filed in support of the motion to reconsider (as proof of a reasonable belief that Jabara was a foreign agent) contained no information that had not been available to defendants throughout the litigation. The district court denied the motion to reconsider because the foreign agent status of Jabara had been in issue and because the information in the additional affidavits had been available to defendants prior to the grant of summary judgment. Defendants contend on appeal that the district court did not even consider, as they contend it should have, the additional *in camera* affidavit of Agent French in making its decision to deny the defendants' motion to reconsider the grant of summary judgment, while Jabara contends that the district court did consider it. It appears to us that the district court only determined that the information contained in these French affidavits had been available all along and did not weigh and determine whether the *in camera* affidavit demonstrated that there was reasonable cause to believe that Jabara was a foreign agent. Since, however, we determine herein that Jabara's fourth amendment rights were not violated when the sum-

⁷ We agreed that, as the record stood at the time the district court granted summary judgment to Jabara, it did not support reasonable cause to believe that Jabara was a foreign agent when the FBI requested the affidavits from the NSA.

maries of his overseas telegraphic messages were furnished to the FBI irrespective of whether there was reasonable cause to believe that he was a foreign agent and whether there is a foreign agent exception to the warrant requirement, we need not consider the question whether the district court abused its discretion in not weighing the contents of the *in camera* French affidavit and whether the affidavit established such reasonable cause.

The district court, in determining that Jabara's fourth amendment rights were violated when the FBI, without a warrant, obtained the summaries of his overseas telegraphic communications, distinguished the holding of the District of Columbia Circuit in *Halkin v. Helms*, 598 F.2d 1 (1978). There the court held (see note 5 herein at page 5) that application of the state secret privilege required dismissal of plaintiffs' claims based on alleged interception by the NSA of their overseas communications because the fact of interception need not be and was not divulged. Here, on the other hand, defendants had divulged the interception and later transmittal to the FBI.⁸ Thus, the district court reasoned, the state secret privilege was no impediment to the adjudication of Jabara's fourth amendment claim. The district court went on to hold, citing *Katz v. United States*, 389 U.S. 347 (1967), that the fourth amendment was implicated since Jabara had a reasonable expectation of privacy with respect to his overseas telegraphic communications. The district court further held that, since the record, classified or otherwise, did not reveal evidence that Jabara was a foreign agent or was acting in collaboration with a foreign agent, even if there is a foreign agent exception to the warrant requirement, the exception could not be applied here. The district court therefore granted summary judgment and injunctive relief to Jabara. 476 F.Supp. at 577-579.

As heretofore stated, Jabara does not contend on appeal that

⁸ As pointed out in *Halkin*, 598 F.2d at 8, it is not significant why this disclosure was made by the defendant or the NSA.

the NSA's interception of his foreign telegraphic communications violated his fourth amendment rights, and therefore we may take as a given the proposition that the NSA lawfully received and was in possession of the communications. From this proposition defendants argue, we think correctly, that Jabara's fourth amendment rights were not violated when the summaries were turned over to the FBI because this was not a "search" or "seizure" within the meaning of the amendment. This is a clear implication of such decisions as *United States v. Gargotto*, 476 F.2d 1009 (6th Cir. 1973), cert. denied, 421 U.S. 987 (1975). There an arson investigator gathered some papers from the floor of the burned building as evidence of the cause of the fire. These papers were later turned over to federal agents when they appeared to be gambling records. The court held that the papers were lawfully in the possession of the arson investigator under the "plain view" exception. It further held that the federal agents lawfully obtained possession from the arson investigator, stating (476 F. 2d at 1014):

Evidence legally obtained by one police agency may be made available to other such agencies without a warrant, even for a use different from that for which it was originally taken. *Gulart v. United States*, 387 F.2d 307 (8th Cir. 1967), cert. denied 390 U.S. 1044, 88 S.Ct. 1645, 20 L.Ed.2d 307 (1968).

The holding by our court in *Gargotto* was followed by our court in *United States v. Lewis*, 504 F.2d 92, 104 (6th Cir. 1974), cert. denied, 421 U.S. 975 (1975).

Jabara contends, however, that there was a "search" or "seizure" when the summaries were turned over by the NSA to the FBI under the holding in *Walter v. United States*, 447 U.S. 649 (1980). There some pornographic 8-millimeter films, in boxes that were in sealed packages, were misdelivered after shipment, and the recipient opened the packages. On the boxes were descriptions and drawings that clearly indicated their contents. The recipient, however, did not view the films.

but turned them over to an FBI agent. FBI agents, then, without a warrant, viewed the films with a projector. The question before the Court was whether the films should have been suppressed because the showing of the films with a projector was an illegal search under the fourth amendment.

In a five-to-four decision, the Court held that the showing of the film with a projector was a "search" and therefore the showing violated the fourth amendment. Justice Stevens authored the lead opinion for the majority, saying (447 U.S. at 654):

[N]otwithstanding that the nature of the contents of these films was indicated by descriptive material on their individual containers, we are nevertheless persuaded that the unauthorized exhibition of the films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy. It was a search; there was no warrant; the owner had not consented; and there were no exigent circumstances.

It is perfectly obvious that the agents' reason for viewing the films was to determine whether their owner was guilty of a federal offense. To be sure, the labels on the film boxes gave them probable cause to believe that the films were obscene and that their shipment in interstate commerce had offended the federal criminal code. But the labels were not sufficient to support a conviction and were not mentioned in the indictment. Further investigation—that is to say, a search of the contents of the films—was necessary in order to obtain the evidence which was to be used at trial.

The fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents. Ever since 1878 when Mr. Justice Field's opinion for the Court in *Ex parte Jackson*, 96 US 727, 24 L. Ed 877, established that sealed packages in the mail cannot be opened without a warrant, it has been settled that an officer's authority to possess a package is distinct from his authority to examine its contents.

(Citations and footnotes omitted).

In the instant case, on the contrary, Jabara's very words, summaries of which were supplied to the FBI, had been lawfully intercepted by and were in the records of the NSA. NSA therefore already had in its records, after it intercepted, all that it supplied to the FBI. Jabara appears to argue, however, that the fact that the NSA acquired, stored and retrieved a large amount of information using sophisticated, high-technology methods and equipment should lead to the conclusion that the NSA's acquisition of Jabara's telegraphic messages was not a search and that the only search occurred when, at the request of the FBI, the NSA retrieved Jabara's messages and delivered summaries to the FBI. There are two difficulties with this argument. First, the simple fact remains that the NSA lawfully acquired Jabara's messages, and these are all that it delivered to the FBI. Second, to the extent that Jabara relies on alleged facts surrounding the methods and technology of acquisition, storage and retrieval of information, such as, as was held by the district court, subject to the state secret privilege. It was recognition of the effect of the privilege that caused the district court to limit its consideration to the question whether the targeting of Jabara's communications by the FBI, in obtaining the summaries from the NSA, was a fourth amendment violation irrespective of the facts surrounding the acquisition, storage and retrieval of the information by the NSA.

Jabara, however, would have us apply still another analysis in support of his contention that his fourth amendment rights were violated when the FBI, without a warrant, requested and received summaries of his overseas messages. In this connection he relies on such cases as *United States v. Bailey*, 628 F.2d 938 (6th Cir. 1980). In *Bailey*, government undercover officers delivered a drum of a chemical, a precursor for the manufacture of a controlled substance, to defendant. The officers had installed a "beeper" inside the drum to aid in ~~the surveillance and investigation of a suspected clandestine~~

laboratory. The signal from the beeper was used by the officers to ascertain the location of the drum. The question raised was whether the placing of the beeper in the drum before it was delivered to defendant and the subsequent tracing of the drum by receipt of the signal from the beeper implicated the fourth amendment. In reaching the conclusion that the fourth amendment was implicated, our court, relying on *Katz v. United States*, 389 U.S. 347 (1967), held that the question was whether defendant had a reasonable expectation of privacy with respect to the location of the drum. In this connection, our court stated (628 F. 2d at 940):

We consider it irrelevant whether a particular governmental intrusion is classified as a "search" or as a "seizure." What matters is whether it violates an individual's legitimate expectation of privacy. Therefore, it is not necessary to speculate whether a beeper "searches" or "seizes" anything.

Our court then quoted (628 F.2d at 941) from Justice Harlan's concurring opinion in *Katz* to the effect that, while a reasonable expectation of privacy is the test, this means that the person asserting the claim must have exhibited an actual (subjective) expectation of privacy and that the expectation must be one that society is prepared to accept as reasonable.

Applying this analysis utilized by our court in *Bailey*, we agree that Jabara exhibited an actual (subjective) expectation of privacy when he sent the telegraphic messages overseas. But the question here is whether he had an expectation of privacy that society is prepared to recognize as reasonable after the messages had lawfully come into the possession of the NSA. For it was after the messages were intercepted and within the possession of the NSA and only when they were delivered to the FBI that Jabara contends that his fourth amendment rights were violated. We do not believe that an expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant

rant, to another government agency is an expectation that society is prepared to recognize as reasonable. In this connection, we believe that it is irrelevant that Jabara did not know that the NSA had intercepted his messages. To hold otherwise would in many instances require, for fourth amendment purposes, a succession of warrants as information, lawfully acquired, is passed from one agency to another.

We conclude, therefore, that Jabara's fourth amendment rights were not violated when the FBI obtained summaries of his overseas telegraphic communications from NSA and that the district court erred in granting summary judgment to Jabara and that, on the contrary, it should have granted summary judgment to defendants as to this claim.⁹

III.

The district court also granted summary judgment to Jabara with respect to his claim that the FBI had violated a provision in the Privacy Act, 5 U.S.C. § 552a(e)(7), which provides that an agency shall:

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or *unless pertinent to and within the scope of an authorized law enforcement activity.*

(Emphasis added).

In construing the emphasized words in this statute, the district court concluded (476 F.Supp. at 581):

Given this definition, it is difficult to conclude that the self-contained exemption in § 552a(e)(7) relating to law

⁹ In note 5, *Halkin v. Helms*, 598 F.2d at 4 (D.C. Cir. 1979), it is pointed out that, as a result of Exec. Order No. 12096, 43 Fed. Reg. 5673 (1978), requests such as that made by the FBI here are screened by a Policy Review Committee of the National Security Council and must be validated as legitimate foreign intelligence needs.

enforcement activity applies to any records which do not relate to specific past, present or future criminal acts.

The district court then determined, based upon the record before it, that the FBI's investigation that involved Jabara's first amendment activities did not relate to specific past, present or future criminal acts.

It thereupon entered an order providing that (App. at 197):

Defendants and their successors in office are enjoined from recording, maintaining, using or disseminating information about the Plaintiff's political beliefs, communications, speeches, writings, associations or activities, both public or private, which do not relate to specific criminal acts.

Defendants then submitted the motion to reconsider the grant of summary judgment to Jabara on the claimed violation of the Privacy Act, which motion was supported by legislative history with respect to this statutory provision and by the aforementioned French open and *in camera* affidavits with respect to defendants' contention that, at least after November 1, 1971, the FBI had reasonable cause to believe that Jabara was a cadre member of a Middle East terrorist organization. The district court denied the motion to reconsider, stating that the defendants were tardy, without excuse, in supplying the legislative history and that, again, the facts set out in the French affidavits were known to the defendants prior to the grant of summary judgment.

Defendants contend that the legislative history demonstrates that the exemption in § 552a(e)(7) ("unless pertinent to and within the scope of an authorized law enforcement activity") allows investigation with respect to the exercise of first amendment rights if such investigation is relevant to an authorized criminal investigation or to an authorized intelligence or administrative one (Defts' brief at 36).

~~Jabara reads the legislative history similarly and comes close~~

to agreeing with defendants' construction of the exemption in the statute, stating:

By its terms and legislative history the subsection does not bar the maintenance of records describing how a person exercises First Amendment rights if there is a direct nexus to an authorized criminal, civil or administrative law enforcement activity.

(Jabara's brief at 39-40).

We agree with both Jabara and the defendants that the district court's construction of the exemption in the statute, limiting it to investigation of past, present or future criminal activity, is too narrow. Moreover, if there is any difference of substance between Jabara's formulation and defendants' formulation of the effect of the exemption, we believe that the defendants' is, in the light of the legislative history, the more reasonable one.

It appears, then, that in granting summary judgment to Jabara on the Privacy Act claim, the district court applied too narrow a test in determining that the FBI's investigative conduct did not come within the statutory exemption. For this reason, we believe that the summary judgment should be vacated and the case remanded to the district court for application of a correct legal standard. In doing so, the district court, of course, is free to reconsider its prior decision not to consider and weigh the effect of the French *in camera* affidavit.

The judgments of the district court are therefore vacated and the case is remanded for further proceedings not inconsistent with this opinion.

No. 55,963

STATE OF KANSAS,
Plaintiff-Appellant,

v.

TIMOTHY RAY HOWARD,
and
ROSEMARIE HOWARD,
Defendants-Appellees.

SYLLABUS BY THE COURT

1.

The term "wire communication," as defined in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. § 2510), is construed to apply only to that portion of a radio telephone conversation which is actually transmitted by wire and not broadcast in a manner available to the public.

2.

That portion of a cordless telephone conversation intercepted by an ordinary FM radio does not fall into the category of a "wire communication," but is to be considered as an "oral communication" subject to the rules pertaining to the interception of oral communications prescribed in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

3.

Owners of a cordless telephone located in a private residence who had been fully advised by the owner's manual as to the nature of the equipment, which involves the transmission and reception of FM radio waves, had no reasonable expectation of privacy. Hence,

police officials could lawfully monitor and tape-record conversations of the owners heard over an ordinary FM radio, and such conversations were admissible in evidence in a criminal action charging the owners with narcotic drug violations.

4.

The utilization of a pen register does not violate the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. § 2510 et seq.).

Appeal from Reno district court; WILLIAM F. LYLE, JR., judge. Opinion filed March 24, 1984. Reversed and remanded.

David E. (Rick) Roberts, assistant county attorney, argued the cause, and Robert T. Stephan, attorney general, and Timothy J. Chambers, county attorney, were with him on the brief for the appellant.

Herbert R. Hess, Jr., of Hess, Leslie & Brown, of Hutchinson, argued the cause and was on the brief for the appellees.

the informant with a tape recorder and a number of blank tapes, requesting the informant to record any further conversations heard over the radio and to record the time of the conversations. Law enforcement officers then obtained court authorization to install a pen register on defendant's telephone. A pen register is a mechanical device which records only the numbers dialed on a telephone by monitoring the electrical impulses caused by use of the telephone's dial or push buttons, but which do not overhear oral communications or indicate whether calls are actually completed. The records maintained by the informant as to the times of recorded conversations corresponded with the records maintained by the pen register. All calls recorded by the informant originated in the home of the defendant. The parties stipulated that the recordings made by the confidential informant were not obtained with the consent of either defendant or the consent of other parties to the conversations. The law enforcement authorities did not obtain an order from a court authorizing them to monitor or record the conversations originating from defendants' residence.

The informant recorded conversations of defendants from July 13, 1982, until August 21, 1982. Based primarily upon the information received from the tape recordings, a search warrant was obtained to search defendants' residence for the cordless telephone in question as well as items of contraband. This search warrant was also based in part upon recordings of the pen register mentioned above and personal observations of the movements of the defendants. Agent Bradley testified that he would not have attempted to obtain a search warrant based solely upon the first tape recordings prepared by the confidential informant which were obtained without the police officers' knowledge or involvement. The search warrant was executed, and the search disclosed a cordless telephone and certain narcotic drugs which were seized by law enforcement personnel within the defendants' residence.

The opinion of the court was delivered by

PRAGER, J.:

This is a criminal action in which the defendants, Timothy Ray Howard and Rosemarie Howard, were charged with possession of cocaine (K.S.A. 65-4127a) and conspiracy to sell marijuana (K.S.A. 21-3302 and K.S.A. 1982 Supp. 65-4127b). The State has taken an interlocutory appeal, pursuant to K.S.A. 22-3603, from an order of the district court suppressing certain taped conversations and other evidence obtained by the police authorities following a search of the defendants' house in Hutchinson. The district court held that the interception of defendants' cordless telephone conversations and the tape recording thereof were in violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 which may be found at 18 U.S.C.A. § 2510 et seq.

For purposes of this appeal, the facts are undisputed and were found by the trial court to be as follows: A neighbor of defendants, referred to in the record as a confidential informant, was operating his AM/FM radio and, in the process of turning the tuning dial, suddenly began to hear conversations over the radio. He determined that the voices were those of the defendants who were conversing with others through use of a cordless telephone. The radio receiver in question was a standard make and model and had not been modified in any manner to monitor or intercept defendants' conversations. The radio was located at all times within the physical confines of the informant's residence without the knowledge of and without direction from law enforcement officers. The informant tape recorded one or more of these conversations. He then provided information about the conversations to law enforcement officers who directed the information to Floyd Bradley, a Kansas Bureau of Investigation (KBI) agent. The conversations were of interest to the KBI, because they involved narcotic drugs. Bradley provided

same or similar frequency utilized by commercial FM radio stations. A standard FM radio would be able to pick up the radio transmissions from both the mobile and base units of the cordless telephone.

The FM signal transmitted from either the base or mobile unit is nondirectional and will reach out in all directions simultaneously. The FM signal transmitted will penetrate and pass through almost any material, including a normal concrete or wooden wall. The effective rated range of communication between a mobile and base unit is approximately 50 feet, but this range varies with the physical surroundings in which the particular cordless telephone is situated. The range varies with the physical surroundings, weather conditions, the sensitivity of the receiver, and the power output of the transmitter. The manual states that, although the cordless telephone is designed for a normal range of 50 feet, the range can vary from anywhere between 30 feet to 100 feet depending upon the particular surroundings.

The manual states that "walkie-talkies" can share the same frequencies of the cordless telephone which can produce some interference. If two cordless telephones were hooked to separate lines and were physically close enough, calling one telephone would cause the second telephone to ring and both telephones would be privy to the same conversation. The only way to correct this situation would be to return the cordless telephone to its place of manufacture for frequency modifications. The cordless telephone in question is required to pass Federal Communications Commission regulations which are limited to compliance with production specifications and not transmission capabilities. One is not required to have a license to operate either the base or the mobile unit because the power of each unit is less than one watt. Hutchison testified that the hand-held mobile unit contains a "confidential" button. When that button

At the hearing on the motion to suppress, James Hutchison, an employee of Carden's Radio Shack in Hutchinson, testified as to the nature and operational dynamics of the cordless telephone. The cordless telephone was manufactured by the Radio Shack Corporation. It works much like a CB radio. It consists of a base unit and a mobile unit. The base unit is physically attached to two separate wires, one of which is the land based telephone line and the second of which is an AC power source. The mobile unit is a self-contained unit with its own batteries which are recharged when the mobile unit is physically rested upon the base unit. No cord or line or physical connection of any kind exists between the mobile unit and the base unit. The mobile unit is much like a conventional telephone and one can both hear from and speak into the mobile unit. Communication between the base unit and the mobile unit takes place through the reception and transmission of FM radio signals by both the base and mobile units.

At the hearing, defendants introduced into evidence the owner's manual for the cordless telephone. Hutchison testified that an average customer would be able to determine from the manual that the device in question was a radio transmitter and receiver. He based this conclusion upon the information contained in the manual. The manual sets forth the transmitted frequencies and the received frequencies of both the base unit and the portable handset. The manual differentiates between the telephone and radio aspects of the cordless telephone by separating the telephone specifications from the radio transmission and reception specifications. Reference is made to the "antenna" of the mobile unit. The mobile and base unit communicate with each other by means of FM radio signals. The FM signal utilized by both the mobile and base units is the same as any other FM signal and is not specialized in any way. The FM signal utilized is of the

is depressed, a person holding the telephone could talk to others in the immediate vicinity without having his voice broadcast over the hand-held unit. This would also allow the operator of the hand-held unit to hear incoming transmissions but not to broadcast from the unit.

The trial court adopted the above facts with additional findings that the conversations taped initially by the neighbor, which were delivered to agent Bradley, would not have been sufficient for the issuance of a search warrant in the case, and that all recorded conversations of the defendants took place while the defendants were in their private residence and talking on the cordless telephone installed in that residence. The trial court, in suppressing the evidence, held that Title III of the Omnibus Crime Control and Safe Streets Act of 1968 controlled the result in this case and that the provisions of the act were violated so as to require suppression of the evidence. The parties to the appeal are in agreement that Title III is controlling and that its provisions must be applied in this case.

At the outset, it would be helpful to briefly summarize the provisions of Title III which may be found at 18 U.S.C.A. § 2510 et seq. The Kansas statutes, K.S.A. 22-2514 et seq., covering eavesdropping and wiretapping, have incorporated specifically and comply with the provisions of Title III. 18 U.S.C.A. § 2510 is the definitive section and defines the key terms. It provides in part as follows:

"§ 2510. Definitions

"As used in this chapter --

"(1) 'wire communication' means any communication made in whole or in part through the use of facilities for

the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications;

"(2) 'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation;

"(4) 'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.

"(5) 'electronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire or oral communication other than --

"(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

"(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

. . . .

"(11) 'aggrieved person' means a person who was a party to any intercepted wire or oral communication or a person against whom the interception was directed."

Section 2511 prohibits the unlawful interception or disclosur

has been made, the court then determines whether or not an improper form of interception has taken place.

There are a number of cases which discuss the purpose of Title III and the ends which Congress sought to achieve thereby. In United States v. Carroll, 332 F.Supp. 1299 (D.C. Cir. 1971), it is stated that Title III was intended to deal with increasing threats to privacy resulting from the growing use of sophisticated electronic devices and the inadequacy of the limited prohibitions contained in the early communications act, 47 U.S.C. § 605. In United States v. Cianfrani, 573 F.2d 835, 855 (3rd Cir. 1978), it is stated that Title III has a twofold purpose: (1) to protect the privacy of oral and wire communications, and (2) to provide on a uniform basis the circumstances and conditions for the interception of such communications. It has been said that the statute is deemed to be the legislative enactment of the Fourth Amendment exclusionary rule and its purpose is to deter the invasion of an individual's privacy through the misconduct of officials by denying the fruits of their transgressions. In Re Proceedings to Enforce Grand Jury Subpoenas, 430 F.Supp. 1071 (E.D. Pa. 1977).

The provisions of Title III have been applied in cases involving a wide variety of factual circumstances. The problem presented in the case now before us is to apply Title III to a case involving a cordless telephone. The courts which have dealt with this specific problem have not been in agreement and have arrived at contrary conclusions. In United States v. Hoffa, 436 F.2d 1243 (7th Cir. 1970), cert. denied 400 U.S. 1000 (1971), FBI agents overheard calls made by defendant Hoffa placed from mobile telephone units located in automobiles owned by the union. They were monitored at the Detroit FBI office by means of ordinary commercial-type FM radio receivers. The court held that defendant had no

of wire or oral communications and provides a penalty of fine or imprisonment for violation of the section. Section 2512 prohibits the manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices. Section 2513 provides for the confiscation of wire or oral communication intercepting devices. Section 2515 prohibits the use of evidence of intercepted wire or oral communications in the following language:

"Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."

Sections 2516 through 2519 provide a procedure for the obtaining of judicial authority for the interception of wire or oral communications, for the disclosure and use of such communications, and for the making of reports concerning such communications. Section 2520 provides that any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall have a civil cause of action and may recover damages against any person who violates the provisions of the act. It should also be noted that specific exceptions are set forth throughout the definitional section, 18 U.S.C.A. § 2510, and throughout the balance of Title III which provide that certain types of interceptions will not be deemed unlawful. In cases where the issue of the application of Title III is involved, the standard procedure is for the court to first proceed to examine the facts in light of the definitions found at 18 U.S.C.A. § 2510. Once this examination

expectation of privacy protected by the Fourth Amendment as to calls which originated from the mobile telephone in the automobile where the calls were exposed to everyone in that area who possessed an FM radio receiver or another automobile telephone tuned in to the same channel. The court cited Alderman v. United States, 394 U.S. 165, 22 L.Ed. 2d 176, 89 S.Ct. 961 (1969); and Katz v. United States, 389 U.S. 347, 19 L.Ed. 2d 576, 88 S.Ct. 507 (1967).

The issue arose again and was determined in a contrary manner in United States v. Hall, 488 F.2d 193 (9th Cir. 1973). There defendant Hall and others were charged with possession of marijuana with intent to distribute. Hall had radio-telephones installed in two automobiles. In early April 1971, a Tucson housewife, who listened to her radio while doing housework, intercepted the appellant's conversations on her radio, which was not unique. After eavesdropping for less than a month, she reported what she considered to be suspicious conversations to the Arizona Department of Public Safety. She continued to monitor the conversations and made reports to the department until May 21, 1971, when the department began its surveillance. For five weeks thereafter, the Arizona Department of Public Safety conducted warrantless electronic surveillance of the appellants' conversations which led to their arrests. The Court of Appeals held that Title III was the controlling statute in the case. It stated that if the interception in question fell within the parameters of Title III, the warrantless surveillance must be suppressed. The court stated that the threshold question was whether these radio-telephone conversations constituted an "oral communication" or a "wire communication." The answer was critical because the definition of oral communication includes the expectation of privacy language derived from Katz v. United States. In order for an oral com-

munication to be protected by the Act, the speaker must have "an expectation that such communication is not subject to interception under circumstances justifying such expectation" 18 U.S.C.A. § 2510 (2).

The court noted that a "wire communication" has no such restriction in its definition. It is defined in 18 U.S.C.A. § 2510(1) as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." The reason for the differentiation between a wire communication and an oral communication was stated in the following language:

"Obviously, there is a reason for the more restrictive definition of oral communications. When a person talks by telephone, he can reasonably assume privacy. That assumption may often be invalid for non-wire communications. Therefore, it is incumbent upon the participants in an oral communication to make a reasonable estimate of the privacy afforded them by their particular circumstances.

"The definition of wire communication is not free from ambiguity. '[C]ommunication made in whole or in part . . . through the use of facilities . . . by the aid of wire . . . between the point of origin and the point of reception . . .' could be interpreted in several ways. For example it could be argued that if any wire is used to aid the communication, it must be deemed a wire communication. If this were followed to its conclusion, the use of a radio would be included in the definition because some wires are contained in the radio transmitter and receiver--thus the communication would be aided 'in

part' by the use of wire. However, such an interpretation would be inconsistent with the language of the immediately succeeding section which permits an agent of the FCC, in certain circumstances, 'to intercept a wire communication, or oral communication transmitted by radio'

18 U.S.C. § 2511(2)(b).

"Broadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire. As with any broadcast into the air, the invitation to listen is afforded to all those who can hear. In the instant case, the eavesdroppers merely tuned their radio receivers to the proper station. It is obvious that conversations initiated from a radio-telephone more logically fall within the category of 'oral communication.'

"By reading the sections together, we can only conclude that the Congress did not mean that every conversation aided in any part by any wire would be a wire communication. As a radio broadcast must be deemed an oral conversation, we believe it would strain the legislative intent to hold that conversations emanating from a radio telephone would not be treated similarly." pp. 196-97.

The court in Hall thus reasoned that conversations emanating from a radio-telephone should logically be treated in the same way as an oral communication.

The court then noted some of the conversations were between two radio-telephones while others were between a radio telephone and a regular land-line telephone. It stated that while the former are within the definition of oral communications, the use of a land-line telephone at one end of the conversation raises a serious question

as to the defined category in which such a communication belongs. The court stated that while logic may dictate the same rule should apply when a conversation crosses the airways but initiates or terminates on a land line, it was not free to reach that result if the legislative intent is to the contrary. In view of the definition of "wire communication" in 18 U.S.C.A. § 2510(1), which was an indication of Congressional intent, it was forced to conclude that, "when part of a communication is carried to or from a land-line telephone, the entire conversation is a wire communication and a search warrant is required." p. 197.

The court then proceeded to criticize its final conclusion, stating that it realized that its classification of a conversation between a mobile and land-line telephone as a wire communication produced what it considered to be an absurd result. It noted that these conversations were intercepted by an ordinary radio receiver and not by a phone tap. Logically, they should be afforded no more protection than those occurring between two radio transceivers. They should be oral communications. However, Congress's definition of a wire communication necessitated the conclusion that the communications were wire communications. The court also observed that there was nothing in the legislative history of Title III to indicate how Congress intended to treat a radio-telephone conversation. It concluded that, in the absence of such an indication, if a conversation involves a land-line telephone, it is a wire communication. It suggested that if any changes were to be made in the law, it was up to Congress. The court held, however, that conversations not involving a land-line telephone, were oral communications, not "wire communications." Because such oral conversations lacked the requisite expectation of privacy, prior authority to intercept was not required by the statute as to those conversations.

Several years after the decision in United States v. Hall, the Supreme Court of Florida had before it a case involving a telephon beeper communication. In Dorsey v. State, 402 So. 2d 1178 (Fla. 1981) the defendant's arrest stemmed from an investigation by the St. Petersburg police department into the operation of a narcotics ring headed by one John Bailey. The investigation began with the use of a paid informant, whose information prompted the police to monitor, by means of a radio scanner, messages received by Bailey and others on a "pocket pager" or "beeper" rented by Bailey. The beeper was a type of pocket pager which a person carries on his person and through which he may receive messages. This is accomplished when another person dials the telephone number of the company that distributes the beepers. The calling party hears a tone and thereafter has ten seconds in which to announce his message. This message is then converted into radio waves and transmitted to the party with the beeper and to any member of the public who has a radio tuned to this frequency. The receiving party can only listen to the message, since the beeper is a receiver and not a transmitter. A "bearcat scanner," capable of receiving any programmed frequency, was used by the police to intercept these beeper messages. The defendants contended that a court order was necessary to legally intercept these communications under the Florida statutes which corresponded in relevant parts with those set forth in Title III. Since a court order was not obtained, the defendants contended that there was a wiretap and that all evidence acquired therefrom was also illegal and must be suppressed.

The Florida court recognized, but rejected, the decision in United States v. Hall. The court followed a well-settled rule in Florida that statutes must be construed so as to avoid absurd results. It then construed the Florida statute to avoid reaching a result that would require police officials to obtain a warrant or a

court order to listen to the open and available airwaves. The court stated that the definition of "wire communications" must be interpreted in a common sense and reasonable manner. It held that the prohibition of interception of wire communications "made in whole or in part through the use of facilities for the transmission or communications by the aid of wire" applied only to so much of the communication as is actually transmitted by wire and not broadcast in a manner available to the public. It noted that, just as it would be absurd to include within the definition of "wire communication" a message broadcast over a public address system for every one to hear, even though the communication is aided by certain wires, it would be equally absurd and asinine to include within that definition television or radio signals broadcast with no reasonable expectation of privacy and openly available for anyone with the proper receiving equipment to hear. The court emphasized the broadcast nature of such messages, and that one who sends beeper messages should know that such communications are open to any members of the public who wish to take the simple step of listening to them. Such signals thus lack any expectation of privacy. They are, by the very nature of being broadcast, communications unprotected by any constitutional right or by the Florida wiretap statute and are thus admissible into evidence.

When we turn to the factual circumstances in the present case as set forth above, it is clear that there was an interception of a communication. The crucial issue we must decide is whether the communications intercepted were "wire communications" or "oral communication," as defined in 18 U.S.C.A. §2510. If the intercepted conversations were "wire communications," then the district court was correct in suppressing the evidence, because no prior court authorization was obtained. If the conversations intercepted were "oral communications," we must determine whether the defendants had a reasonable expectation of privacy under the circumstances.

From our study of the cases and the legislative history of Title III, we have concluded that the conversations in this case which were intercepted between the mobile unit and the base unit of the cordless telephone were not "wire communications" but fall into the category of "oral communications." In our judgment, United States v. Hall not only arrived at an absurd result but misconstrued the Congressional intent. In construing a statute, the fundamental rule of statutory construction, to which all others are subordinate, is that the purpose and intent of the legislature governs when that intent can be ascertained from the statute, even though words, phrases or clauses at some place in the statute must be omitted or inserted. Farm & City Ins. Co. v. American Standard Ins. Co., 220 Kan. 325, Syl. ¶3, 552 P.2d 1363 (1976). In determining legislative intent, courts are not limited to a mere consideration of the language used, but look to the historical background of the enactment, the circumstances attending its passage, the purpose to be accomplished, and the effect the statute may have under the various constructions suggested. Brown v. Keill, 224 Kan. 195, Syl. ¶3, 580 P.2d 867 (1978). In order to ascertain the legislative intent, courts are not permitted to consider only an isolated part or parts of an act but are required to consider and construe together all parts thereof in pari materia. Another principle of statutory construction well recognized is that a statute should never be given a construction that leads to uncertain injustice, or confusion, if it is possible to construe it otherwise. Coe v. Security National Ins. Co., 228 Kan. 624, 620 P.2d 1108 (1980). Furthermore, courts are not bound to an examination of the statutory language alone, but may properly inquire into the causes which impelled the statute's adoption, the objectives sought to be attained, the statute's historical background, and the effect the statute may have under the various constructions suggested. State, ex rel., v. Kalb, 218 Kan. 459, 464, 543 P.2d 872 (1975).

The Supreme Court of the United States has held that a statute should not be given a literal construction, if such constructi

is contrary to the legislative intent and leads to absurd conclusions. United States v. Bryan, 339 U.S. 323, 94 L.Ed. 884, 70 S.Ct. 724 (1950). The United States Supreme Court, like the courts of Kansas, also follows the rule that penal statutes are to be construed strictly. F. C. C. v. American Broadcasting Co., 347 U.S. 284, 296, 98 L.Ed. 699, 74 S.Ct. 593 (1954). It cannot be denied that 18 U.S.C. § 2511, which makes it a crime to intercept or disclose communications in a manner prohibited by the act, is a penal statute. In United States v. Hall, the court recognized this, noting that its holding was ironic, since Title III involves stringent civil and criminal penalties for those who violate its provisions. In other words, the court observed, any citizen who listens to a mobile-telephone band does so at his own risk, and scores of mariners who listen to the ship-to-shore frequency, commonly used to call to a land-line telephone, commit criminal acts.

It seems logical to us that cordless telephone conversations, which may be heard by anyone listening on an ordinary radio receiver, should not be included within the definition of a "wire communication" under Title III. The Congressional purpose in enacting Title III has been discussed above. It was intended to incorporate the Fourth Amendment safeguards in the interception of human communications. United States v. Mainello, 345 F. Supp. 863 (E.D. N.Y. 1972). Title III was designed for a dual purpose--to protect the individual's right of privacy and to provide a uniform and systematic basis for the interception of human communications by the police authorities.

The American Bar Association Standards Relating to Electronic Surveillance § 1.1 declares:

"The objectives of standards relating to the use of electronic surveillance techniques should be the maintenance of privacy and the promotion of justice."

In the general commentary of the Advisory Committee at pages 21-22 of the Standards, it is stated that privacy and justice must be balanced in this area. The following language is used:

"Mr. Justice Frankfurter once observed of journeys in the law that often 'where one comes out on a case depends on where one goes in.' So it is in any examination of the many troublesome questions associated with the use of electronic surveillance techniques in the administration of justice and various proposals for reform. All too often discussions of these questions, however, have tended to degenerate into arid debates between contending ideologies. At one extreme, some seem to believe that the social order depends almost exclusively on the penal law, and requires the capture, conviction and punishment of as many culprits as possible. Society's laws must be vindicated by appropriate expiation or measured deterrence and, if possible, the offender reformed. Privacy may be important, but justice is always paramount. At the other extreme, some seem to think that all criminal law is formalized vengeance, that incarceration is a pointless cruelty without meaning as expiation, deterring or reforming no one, embittering its victims more than it protects society, and inflicting less pain on the guilty than on innocent dependents. Justice is of little importance, while privacy is always paramount. Between these untenable extremes, there is, of course, a middle way. 'The adjustment between the rights of the individual and the rights of the community must depend upon the needs and conditions which exist at any given moment' A system of penal law must maintain, the Advisory Committee believes, both privacy and justice. Neither value can be dogmatically accorded priority. The problem is as the late Judge Learned Hand put it: there is 'no escape in each situation from balancing the conflicting interests

at stake with as detached a temper as we can achieve."
Standards Relating to Electronic Surveillance, pp. 21-22.

After approaching the problem in as detached a temper as we can achieve, we have concluded that the term "wire communication," as defined in 18 U.S.C.A. §2510 (1), should be construed to apply only to that portion of a radio-telephone communication which is actually transmitted by the wire and not broadcast in a manner available to the public. We hold that those portions of the cordless telephone conversations intercepted by an ordinary FM radio in this case did not fall into the category of a "wire communication," but were in fact oral communications and that the rules pertaining to the interception of oral communications prescribed in Title III are applicable.

In the case before us, it is undisputed that there was an interception of an oral communication transmitted by radio. We hold that these defendants, who as owners of the cordless telephone had been fully advised by the owner's manual as to the nature of the equipment, had no reasonable expectation of privacy under the circumstances. We wish to emphasize, however, that this case does not involve the rights of a person on the other end of the telephone land line who was speaking over a standard telephone and who was without knowledge that the defendants were the owners and users of a cordless telephone. In reaching this conclusion, we have followed what we believe to be the Congressional intent in the enactment of Title III--to protect the individual's rights of privacy and also to provide a uniform and systematic method for the interception of human communications by police officials to protect the public from criminal activities. On the basis of this rationale, we hold that the trial court erred in suppressing the intercepted cordless telephone conversations and the evidence obtained pursuant to the search warrant.

The State in this appeal also presents to the court a question as to the admissibility of the recordings of the pen register which was installed by law enforcement personnel after obtaining court authorization for the installation. This issue was raised but not ruled on by the district court. At the hearing, the only evidence presented on this issue was that the pen register was installed by court authority. Under the circumstances, there was no factual basis to challenge the admissibility of the recordings of the pen register. Furthermore, the law is clear that the utilization of a pen register does not violate the provisions of Title III. See United States v. New York Telephone Co., 434 U.S. 159, 54 L.Ed. 2d 376, 98 S.Ct. 364 (1977), where it was held that Title III does not govern the authorization by a federal district court for the installation and use of a pen register by federal law enforcement officers.

For the reasons set forth above, the case is reversed and remanded to the district court for trial or further proceedings.

652 Mich. 308 NORTH WESTERN REPORTER, 2d SERIES

Malcolm in that the present home would be operated by a nonprofit, charitable corporation. The operation of the home in *Jayno Heights* can be distinguished in that it was commercial in nature.

Finally, the basis of affiliation in this case cannot be distinguished from that in *Malcolm* which involved a substantially identical home for six or fewer developmentally disabled adults. Although a residential foster parent was present in the home in *Malcolm*, and it is not clear from the facts of the case at bar whether one would be present in the instant home, we do not deem this distinction to be a significant one. The precept that a parent is the essence of a family does not seem to have been of any importance in either *Bellarmino* or *Malcolm*. In any event, 24-hour supervision is to be provided in the instant home.

Thus, comparing the facts of this case to those in *Bellarmino*, *Jayno Heights* and *Malcolm*, we hold that they more closely resemble *Bellarmino* and *Malcolm*. The present deed restriction prescribes only the building of a single family dwelling in the subdivision, it does not limit its use. However, be that as it may, the residents of defendants' home would constitute "a family" under the holdings of this Court in *Bellarmino* and *Malcolm*.

The lower court order granting plaintiff's motion for summary judgment is vacated. This cause is reversed and remanded and the lower court is instructed to enter an order granting defendants' motion for summary judgment.



107 Mich.App. 78

PEOPLE of the State of Michigan,
Plaintiff-Appellant,

v.

John George DEZEK,
Defendant-Appellee.

PEOPLE of the State of Michigan,
Plaintiff-Appellant,

v.

Robert Eugene MEDEMA,
Defendant-Appellee.

PEOPLE of the State of Michigan,
Plaintiff-Appellee,

v.

Harold THOMPSON,
Defendant-Appellant.

PEOPLE of the State of Michigan,
Plaintiff-Appellee,

v.

Gifford Hall PLETCHER,
Defendant-Appellant.

PEOPLE of the State of Michigan,
Plaintiff-Appellee,

v.

Lester G. KELLY, Defendant-Appellant.

PEOPLE of the State of Michigan,
Plaintiff-Appellee,

v.

Michael D. PETRUSKA, Jr.,
Defendant-Appellant.

Docket Nos. 49011, 47342, 48128, 59700,
50685 and 49827.

Court of Appeals of Michigan.

June 4, 1981.

Released for Publication Aug. 5, 1981.

Defendants were charged with gross indecency between males. Some defendants' motions to suppress were granted by the Circuit Court, Kalamazoo County, Donald T. Anderson and Charles H. Mullen, JJ., while other defendants' motions to suppress

PEOPLE v. DEZEK

Mich. 653

Cite as, Mich.App., 306 N.W.2d 652

were denied by the Court, Robert L. Borsos and Patrick H. McCauley, JJ., and appeals were taken. The Court of Appeals held that: (1) affidavits for video surveillance of restroom in highway rest area where homosexual activity was suspected did not adequately set forth basis for the informant's conclusions or any basis for inferring the credibility of the informant, and (2) warrant did not limit the search to precise and discriminate circumstances.

Order accordingly.

1. Searches and Seizures ⇐7(10)

Bathroom stalls in restroom at highway rest area were temporarily private places whose momentary occupants' expectations of privacy were reasonable, so that surveillance of the stalls was governed by Fourth Amendment requirements. U.S.C.A.Const. Amend. 4.

2. Searches and Seizures ⇐3.6(4)

Affidavits which contained nothing concerning basis of informant's conclusions as to homosexual activity taking place in restroom in highway rest area and which contained nothing from which the credibility of the informant or the accuracy of the information could be inferred were inadequate to support issuance of search warrant authorizing surveillance in restrooms.

3. Searches and Seizures ⇐3.8(2)

Search warrant for restrooms of highway rest area at which homosexual activity was suspected did not limit the search to precise and discriminate circumstances where the warrant authorized surveillance of every occupant of the stalls during the relevant periods and the stalls were kept under constant surveillance through audio and video monitors.

4. Criminal Law ⇐394A(11)

Video recordings of activities taking place in restroom, police surveillance notes of activities observed through the monitor, and testimony of officers as to activities observed through the monitor or upon entry

into the restroom after observations through the monitor were required to be suppressed where the monitoring was pursuant to an invalid search warrant.

Frank J. Kelley, Atty. Gen., Robert A. Derengoski, Sol. Gen., James J. Gregart, Pros. Atty., Michael H. Dzialowski, Asst. Pros. Atty., for the People.

Richard R. Lamb, Kalamazoo, for defendant-appellant in No. 48128.

Franklin W. Schmiede, Kalamazoo, for defendant-appellant in No. 50700.

William R. Oudsema, Kalamazoo, for defendant-appellant in No. 50685.

William R. Farley, Grand Rapids, for defendant-appellant in No. 49627.

Steven L. Rayman, Kalamazoo, for defendant-appellant in No. 48011.

Stephen W. Burness, Kalamazoo, for defendant-appellant in No. 47342.

Before HOLBROOK, P. J., and V. J. BRENNAN and HOTCHKISS,* JJ.

PER CURIAM.

These consolidated cases arise out of police electronic surveillance of a men's restroom at a highway rest area. The surveillance was conducted pursuant to a search warrant which contained the following authorizations:

"A. Beginning at *October 25, 1978* at *10:00 PM* the visual and audio communications may be recorded as described herein.

"B. Communications between unknown males which are expected to be in the nature of solicitations for sexual activity. Further, any and all sexual activities performed between the males in the mens room of the next area located at the rest area on US-181 south of 'D' Avenue in Alamo Township, Kalamazoo County.

"C. Said conversations may include the statements of other persons present at the same time and place.

* R. C. Hotchkiss, 30th Judicial Circuit Judge, sitting on Court of Appeals by assignment pursuant to Const. 1963, Art. 6, Sec. 23, as amended 1968.

suant to Const. 1963, Art. 6, Sec. 23, as amended 1968.

"D. Recording of these acts and conversations will be accomplished by the use of video and audio equipment located in the mens room at the rest area previously described in Section B.

"E. Said recordings shall terminate on November 1, 1978 at 11:59 P.M."

As a result of the surveillance, some 40 persons including these six defendants were arrested and charged with gross indecency between males, M.C.L. § 750.338; M.S.A. § 28.570. Each defendant herein moved to suppress the evidence obtained through the surveillance. In *Medema*, the circuit judge suppressed the evidence after holding that defendant had a reasonable expectation of privacy in the place searched, that there was not probable cause to issue the warrant, and that the warrant did not describe the things to be seized with sufficient particularity. In *Dezek*, the circuit judge suppressed the evidence after holding that there was no statutory authority for a warrant authorizing video surveillance and that defendant was not "forthwith" served with a copy of the warrant as required by M.C.L. § 780.665; M.S.A. § 28.1259(5). In *Thompson*, the circuit judge declined to suppress the evidence after holding that defendant had no reasonable expectation of privacy in the place searched. In *Petruska, Kelly, and Fletcher*, the circuit judge held that defendants had a reasonable expectation of privacy in the place searched but declined to suppress the evidence after holding that the search was conducted pursuant to a valid warrant. The people appeal of right in *Medema* and *Dezek*, while defendants appeal by leave granted in *Thompson, Petruska, Kelly, and Fletcher*.

I

The initial question we must address is whether defendants had a reasonable expectation of privacy in the place searched. See *Katz v. United States*, 389 U.S. 347, 361-362, 88 S.Ct. 507, 511; 19 L.Ed.2d 576 (1967):

"[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his

own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

In concurrence. Justice Harlan observed:

"[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"

"The critical fact in this case is that [o]ne who occupies it, [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted. . . . The point is . . . that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.*, 361, 88 S.Ct. 516.

Testimony revealed that the men's rest room subject to the search warrant was a large room with one door leading to the outside. Within the room were several urinals and wash basins and four toilet stalls. The stalls were constructed of solid partitions elevated from the floor approximately 8-12 inches. The partition did not extend to the ceiling, but a five-foot eleven-inch man could not peer over its top. At the front of each stall was a door of the same height as the side partitions. The doors had been designed with latches, but the latching devices were broken or missing. Persons using the stalls, including defendants, would usually use small rolls of toilet paper wedged into the door cracks to hold the doors closed. A hole had been created in the common side partition between two of the stalls. The hole was approximately six inches in diameter (as stipulated by the parties in three of the cases; the only testimony concerning the size of the hole disclosed that it was six inches in circumference). It was located about waist high. It was alleged that the illegal acts were committed by one participant placing his penis

PEOPLE v. DEZEK

Mich. 655

Cite as, Mich.App., 300 N.W.2d 652

through the hole while standing in one stall and the occupant of the other stall performing fellatio upon him. Surveillance of the two stalls was accomplished by installation of a needle-point video camera lens in the ceiling above the stalls. The lens was directly connected to a video camera situated above the ceiling panels which was connected by cables to a video tape recorder and a video monitor. The recorder and monitor were located in a room separate from the men's rest room. The audio surveillance was concentrated on the same two stalls but picked up most sound within the room. The video monitor provided continuous video and audio coverage of all activity within the two stalls. The sound was not recorded, but the video recorder was turned on by the officers when they observed through the monitor that sexual activity between males was about to occur in the stalls.

[1] We hold that the bathroom stalls here, like the telephone booth in *Katz*, were temporarily private places whose momentary occupants' expectations of privacy are recognized by society as reasonable. See *Bielicki v. Superior Court of Los Angeles County*, 57 Cal.2d 602, 21 Cal.Rptr. 552, 371 P.2d 288 (1962); *Britt v. Superior Court of Santa Clara County*, 58 Cal.2d 469, 24 Cal.Rptr. 849, 374 P.2d 817 (1962); *Brown v. State*, 3 Md.App. 90, 238 A.2d 147 (1968); *State v. Bryant*, 287 Minn. 205, 177 N.W.2d 800 (1970); *Buchanan v. State*, 471 S.W.2d 401 (Tex.Crim.App., 1971); *People v. Triggs*, 8 Cal.3d 884, 106 Cal.Rptr. 408, 506 P.2d 232, 234 (1973); and *Kroehler v. Scott*, 391 F.Supp. 1114 (E.D.Pa., 1975). See also *People v. Abate*, 105 Mich.App. 274, 306 N.W.2d 476 (1981), in which, under circumstances analogous to those presented here, the Court found a toilet stall in a public rest room at a roller skating rink to be a "private place" under M.C.L. § 750.539d; M.S.A. § 28.807(4). Compare also *People v. Hunt*, 77 Mich.App. 590, 259 N.W.2d 147 (1977), in which the Court expressly distinguished the instant situation while holding that defendant had no reasonable expectation of privacy. In *Hunt*, defendant and his female companion had taken exclusive occupancy of a public rest room for over 30

minutes, during which time moans were heard through the rest room door.

Some jurisdictions, while unprepared to recognize a reasonable expectation of privacy where defendant's activities were viewed from a common area of a restroom, nevertheless have indicated that such an expectation of privacy exists under other circumstances. See *Buchanan, supra*, and *Moore v. Florida*, 355 So.2d 1219 (Fla.App., 1978). In this case, reliance upon the visibility of defendant's activities from the common area of the rest room or through the hole to the adjacent stall is misplaced. In *Katz, supra*, the government argued that defendant placed the telephone calls which were recorded by the police from a glass telephone booth in which defendant was visible to the public. The Court rejected that argument, noting that defendant sought to exclude intruding ears rather than intruding eyes when he entered the booth. Thus *Katz* recognized that an expectation of privacy may be partial and yet receive constitutional protection. A stall such as that at issue here obviously does not afford complete privacy, but an occupant of the stall would reasonably expect to enjoy such privacy as the design of the stall afforded.

II

Since we hold that defendants had reasonable expectations of privacy in the place searched, and since no exigent circumstances are proffered for our consideration, the admissibility of the evidence turns on whether the district judge erred in issuing a search warrant. The judge issued the warrant based on affidavits of three members of the Kalamazoo County Sheriff's Department. Relevant portions of those affidavits are reproduced below. One affidavit provided:

"(3) That the affiant was informed of men soliciting for immoral purposes and suspected homosexual activity at the US-181/4' Avenue rest area, Alamo Township, County of Kalamazoo, State of Michigan.

"(4) That on October 22, 1978, the affiant was informed of an investigation to locate, identify, and arrest persons soliciting for and involved in homosexual acts at the US-131/'D' Avenue rest area. That during the course of the investigation, two men were apprehended in the act of committing gross indecency and subsequently charged.

"(5) That on October 24, 1978, the affiant was part of a team of officers assigned to investigate alleged homosexual activity to include soliciting for immoral purposes and homosexual acts at the rest area on US-131 at 'D' Avenue. That upon entering the mens room the affiant observed men loitering in stalls and the mens room proper. One of the men fit the description of a male subject loitering in the mens room on October 22, 1978. That an unidentified male asked the affiant to accompany him to his car. That the same men entered the restroom on numerous occasions, returning to their cars; not starting the motors. Further, the same subjects were seen walking in the parking lot and spending hours at the rest area. That while in the mens room, a male solicited the affiant for immoral purposes and was subsequently arrested and charged in a complaint and warrant for soliciting for immoral purposes, pleading guilty to the charge in the 8th District Court on October 25, 1978."

A second affidavit provided:

"(2) That as a Shift Commander he was informed of criminal activity in the County. That he was further informed men have been loitering in the mens room and parking areas at the US-131/'D' Avenue rest area, Alamo Township, Kalamazoo County. Further, there was information two men were seen leaving a stall located within the mens restroom at the rest area on October 18, 1978. Further, has received information that men have been soliciting for and involved in homosexual acts.

"(3) That on October 22, 1978, with the background information the affiant initiated an investigation into alleged homosexual activity. At approximately 10:00

date, the affiant entered the mens room at the US-131/'D' Avenue rest area making himself familiar with the interior of the mens room. The affiant observed a hole in the partition separating stalls # 1 and # 2, approximately waist high.

"(4) That while in the restroom, the affiant observed two stalls occupied and both occupant's feet facing forward. After pretending to leave the mens room, the affiant observed both sets of feet facing the hole in the partition and smacking, sucking type sounds coming from both booths. Upon investigating further he observed two males committing a homosexual act. Both subjects were subsequently arrested and warrants were authorized for gross indecency between males. Further, the affiant has observed several of the same men and vehicles at the rest area on October 22, 1978 and October 24, 1978."

The third affidavit provided:

"(2) That as part of his regular duties he is briefed on criminal activities in the County. That as part of this briefing your affiant was informed there were men loitering in the mens room at the US-131/'D' Avenue rest area in Alamo Township, Kalamazoo County. Further, there was information that illegal sex acts were being performed between males in the restroom.

"(3) That as part of your affiant's regular duties, he has gone out to the US-131/'D' Avenue rest area to determine whether there are any illegal activities going on. Your affiant has observed numerous local residents loitering in the rest area. The residence of these persons were learned by obtaining drivers licenses from these persons. These persons were told not to loiter in or about the rest areas.

"(4) These activities were witnessed by this officer in May, 1978, while I was assigned to the 11:00 PM to 7:00 AM shift. During the month of May, 1978, there were numerous times when the same individuals were asked to leave the rest area.

PEOPLE v. DEZEK

Mich. 657

Cite as, Mich.App., 388 N.W.2d 652

"(5) Further, your affiant states that the same type of activity as listed in paragraphs # 3 and # 4 were witnessed while on the 11:00 PM to 7:00 AM shift in August, 1978."

[2] In *Aguilar v. Texas*, 378 U.S. 108, 84 S.Ct. 1509, 12 L.Ed.2d 723 (1964), the court held that affidavits supporting a search warrant may be based on hearsay information and need not reflect the direct, personal observations of the affiant but that the magistrate must be informed of some of the underlying circumstances on which the informant based his conclusions and some of the underlying circumstances from which the officer concluded that the informant, whose identity need not be disclosed, was credible or that his information was accurate. See also *People v. Peterson*, 63 Mich. App. 538, 234 N.W.2d 692 (1975); *People v. Johnson*, 68 Mich.App. 697, 243 N.W.2d 715 (1976); and *People v. Staffney*, 70 Mich. App. 787, 246 N.W.2d 364 (1976). Here, each affidavit contained statements from unidentified informants. The affidavits contained nothing concerning the basis of the informant's conclusions and nothing from which the credibility of the informant or the accuracy of the information could be inferred.

[3] In addition to this defect in the underlying affidavits, we cannot say that the warrant limited the search to "precise and discriminate circumstances" as required by the Court for warrants authorizing electronic surveillance in *Berger v. New York*, 388 U.S. 41, 63, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967). Officers acting under the color of the warrant conducted a search which extended to every occupant of the stalls during the relevant period. The stalls were kept under constant surveillance through audio and video monitors. Yet the affidavits did not indicate that every one who used the stalls was likely to engage in illicit activity.

In *People v. Nieves*, 36 N.Y.2d 396, 369 N.Y.S.2d 50, 330 N.E.2d 26 (1975), the court indicated that a warrant authorizing a search of "any person therein" was permissible only if the facts known to the magis-

trate and the reasonable inferences to be drawn therefrom created a substantial probability that the authorized invasion of privacy would be justified by discovery of the items sought from all persons present when the warrant was executed. In *State v. Sims*, 75 N.J. 337, 382 A.2d 638 (1978), the court stated that "presence" is a descriptive fact which satisfies the intent behind the Fourth Amendment only if there is good reason to believe that anyone present at the anticipated scene would probably be a participant in the crime. Even where there is police observation of known lawbreakers operating from a given location, a warrant permitting a search of all individuals found in that location would be impermissible if that location was actually a public place. See also *People v. Tenney*, 25 Cal.App.3d 16, 101 Cal.Rptr. 419 (1972), and *Crossland v. State*, 266 P.2d 649 (Okla.Crim.App., 1954). The warrant here could not authorize the search conducted by the officers.

III

[4] Evidence which is the product of an illegal search is inadmissible as "fruit of the poisonous tree" unless the connection between the lawless conduct of the police and the discovery of the challenged evidence is so attenuated as to dissipate the taint. *Nardone v. United States*, 308 U.S. 338, 60 S.Ct. 266, 84 L.Ed. 307 (1939); *Wong Sun v. United States*, 371 U.S. 471, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963); *United States v. Coccolini*, 435 U.S. 268, 98 S.Ct. 1064, 55 L.Ed.2d 268 (1978). Applying this standard to the instant cases, we hold to be inadmissible video recordings of the activities in the rest room, police surveillance notes on activities observed through the monitor, and testimony of the officers as to activities observed either through the monitor or upon entry into the rest room after observations through the monitor. Defendant Petraitis also argues that his confession should be suppressed. See, for example, *Wong Sun*, *supra*, 371 U.S. 485-486, 83 S.Ct. 418. However, the evidence in the record here is insufficient for us to determine whether the connection between the lawless conduct of

the police and defendant's confession was attenuated. We therefore decline to suppress the confession without prejudice to defendant raising this issue on remand.

In view of our resolution of the foregoing issues, we need not address the other issues raised by appellants. The decisions of the circuit court in *Medema* and *Dezek* are affirmed. The decisions of the circuit court in *Thompson*, *Petruska*, *Kelly*, and *Fletcher* are reversed, and the cases remanded for further proceedings consistent with this opinion.



107 Mich.App. 72

**Frank KURIAKUZ and Great Savings
Market, Plaintiffs-Appellants,**

v.

**COMMUNITY NATIONAL BANK OF
PONTIAC, Defendant-Appellee.**

Docket No. 53434.

Court of Appeals of Michigan.

June 4, 1981.

Released for Publication Aug. 5, 1981.

Action was brought to recover from bank for alleged breach of loan agreement. The Circuit Court, Oakland County, Robert L. Templin, J., dismissed complaint without prejudice, and plaintiff appealed. The Court of Appeals held that any right of action against bank vested in bankruptcy trustee, notwithstanding that right of action was not listed on asset schedule and such right did not revert to bankrupt after close of the bankruptcy estate, i. e., discharge.

Affirmed.

1. Bankruptcy ⇐146

When plaintiff petitioned for voluntary bankruptcy all of his assets, including right

of action, vested in the trustee and such right of action remained vested in trustee during bankruptcy proceedings even though the asset was not listed on the schedule of assets required to be filed with bankruptcy court. Bankr.Act, §§ 70, 70(a), 11 U.S.C.A. §§ 110, 110(a).

2. Bankruptcy ⇐278

Once the right of action vests in a trustee, the only way that a bankrupt may bring suit on that right of action, at least during pendency of bankruptcy proceedings, is by showing abandonment or by receiving permission from the bankruptcy court. Bankr.Act, §§ 70, 70(a), 11 U.S.C.A. §§ 110, 110(a).

3. Bankruptcy ⇐150

A bankrupt may never assert, during pendency of bankruptcy proceedings, that a trustee has abandoned an asset if that asset has not been listed on the assets schedule. Bankr.Act, §§ 70, 70(a), 11 U.S.C.A. §§ 110, 110(a).

4. Bankruptcy ⇐146

Right of action against bank which allegedly reneged on promise to make certain loans after debtor had detrimentally changed his position in reliance thereon vested in bankruptcy trustee notwithstanding that such right of action was not listed on the asset schedule and the right of action did not revert to the bankrupt after close of the bankruptcy estate, i. e., discharge. Bankr.Act, §§ 70, 70(a), 11 U.S.C.A. §§ 110, 110(a).

5. Bankruptcy ⇐372

Since action was dismissed without prejudice on finding that it should have been asserted by bankruptcy trustee, plaintiff could petition bankruptcy court to reopen his estate and if estate was reopened the trustee would have option of pursuing the action or abandoning it or, alternatively, bankruptcy court could give plaintiff permission to bring the action himself. Bankr.Act, §§ 70, 70(a), 11 U.S.C.A. §§ 110, 110(a).

KURIAKUZ v. COMMUNITY NAT. BANK OF PONTIAC Mich. 659

Cite as, Mich.App., 308 N.W.2d 658

Remo Del Greco, Detroit, for plaintiffs-appellants.

Kenneth R. Lango, Troy, for defendant-appellee.

Before BASHARA, P. J., and KAUFMAN and BANKS,* JJ.

PER CURIAM.

Plaintiffs Frank Kuriakuz and Great Savings Market appeal from an August 11, 1980, order entered in Oakland County Circuit Court granting summary judgment, pursuant to GCR 1963, 117, in favor of defendant Community National Bank of Pontiac. This order dismissed plaintiffs' complaint without prejudice.

Plaintiffs filed their complaint on February 26, 1980. The complaint alleged that in 1977 defendant entered into an oral agreement with plaintiff Frank Kuriakuz (who was co-owner of Great Savings Market) whereby defendant was to make certain loans to Kuriakuz so that he could remain in business. It also alleged that plaintiff Kuriakuz detrimentally changed his position in reliance on this oral agreement and that the loan was subsequently denied by defendant without notice or satisfactory explanation.

Kuriakuz contends that he was forced into bankruptcy because of his detrimental reliance. As one of its affirmative defenses, defendant alleged that plaintiff Kuriakuz is an adjudicated bankrupt, and, therefore, not the owner of the claim which forms the basis of this lawsuit. Defendant maintained that only the trustee in bankruptcy could assert this claim.

Attached as an exhibit to defendant's motion for summary judgment was plaintiff Kuriakuz's voluntary petition for bankruptcy, filed in November of 1978, and the schedules listing all of his assets.

The sole issue raised on appeal is whether a bankrupt is barred from bringing suit on a right of action which accrued prior to his filing for bankruptcy where the bankrupt

did not disclose the right of action on the asset schedules filed with the bankruptcy court.

Section 70(a) of the old Bankruptcy Act, 11 U.S.C. § 110(a), provided in pertinent part:

"(a) The trustee of the estate of a bankrupt and his successor or successors, if any, upon his or their appointment and qualification, shall in turn be vested by operation of law with the title of the bankrupt as of the date of the filing of the petition initiating a proceeding under this title, except insofar as it is to property which is held to be exempt, to all of the following kinds of property wherever located * * * (6) rights of action arising upon contracts, or usury, or the unlawful taking or detention of or injury to his property * * *."

[1] When plaintiff Kuriakuz filed his petition for voluntary bankruptcy, all of his assets, including the right of action which forms the basis of the instant suit, became vested in the trustee in bankruptcy by operation of law. Section 70. This right of action remained vested in the trustee during pendency of the bankruptcy proceedings; even though the asset was not listed on the schedule of assets plaintiff Kuriakuz was required to file with the bankruptcy court. See, e. g., *Moore v. Slonim*, 426 F.Supp. 524, 527-528 (D.Conn.1977), *aff'd* 562 F.2d 38 (CA 2, 1977); *Scharmer v. Carrollton Manufacturing Co.*, 525 F.2d 95 (CA 6, 1975); *In re Thomas*, 204 F.2d 788 (CA 7, 1953).

[2, 3] Once a right of action vests in a trustee, the only way that a bankrupt may bring suit on that right of action, at least during the pendency of the bankruptcy proceedings, is by showing abandonment or by receiving permission from the bankruptcy court. See *Taylor v. Swirnow*, 80 F.R.D. 79, 82 (D.Md.1978); *Riverside Memorial Museum, Inc. v. Umet Trust*, 460 F.Supp. 622

* J. L. Banks, 8th Judicial Circuit Judge, sitting on Court of Appeals by assignment pursuant to

Const. 1963, Art. 6, Sec. 23, as amended 1980.

APPLICATION OF ORDER AUTH. INTERCEPTION, ETC.

421

Cite as 513 F.Supp. 421 (1980)

and Arbuckle's motion for judgment notwithstanding the verdict and for a new trial. Many of the issues raised in these motions have already been addressed by the Court, and to the extent they have not, they warrant little exposition. Suffice it to say that the Court finds all the post-trial motions filed by Plaintiffs in this case to be without merit, and to the extent that the Court has not already made it clear, all these motions should be overruled.

It is therefore ORDERED that INA's motion to dismiss for want of jurisdiction, motion for judgment, or alternatively for judgment notwithstanding the verdict, motion to reopen the evidence, and motion for new trial be and hereby are in all things denied.

It is further ORDERED that Arbuckle's motion for judgment notwithstanding the verdict and motion for a new trial be and hereby are in all things denied.

Judgment shall be entered in accordance with this opinion.



In the Matter of An Application of the United States for an ORDER AUTHORIZING INTERCEPTION OF ORAL COMMUNICATIONS AND VIDEO-TAPE SURVEILLANCE.

MDB No. 80-353.

United States District Court,
D. Massachusetts.

Aug. 15, 1980.*

Upon application by the United States for an order authorizing interception of oral communications and video surveillance, the

* This memorandum was impounded by order of the court until May 8, 1981, when the court granted the government's motion to lift the impoundment order so that this memorandum,

District Court, Keeton, J., held that application would be granted, where substantive safeguards at least as rigorous as those required by title providing for interception of oral communications had been observed and, moreover, application represented that agents implementing video surveillance would be directed that video surveillance component be turned on after it had been determined from the audio component that communications involving illegal activities or illegal activity itself, within scope of the proposed investigation, was taking place and that the video component remain on only as long as and under the same constraints as were imposed on oral interception for the purpose of minimizing the intrusion consistently with the requirements of such title.

Ordered accordingly.

1. Statutes ⇐ 184

When Congress has not directly addressed and answered a question, courts in answering question by necessity, should nevertheless be guided by the aims, principles and policies that manifestly underly enacted statutes.

2. Telecommunications ⇐ 496

Court would grant application for video surveillance, where substantive safeguards at least as rigorous as those required by title providing for interception of oral communications had been observed and, moreover, application represented that agents implementing the video surveillance would be directed that the video surveillance component be turned on after it had been determined from audio component that communications involving illegal activities or illegal activity itself, within scope of the proposed investigation, was taking place and that the video component remain on only as long as and under the same constraints as were imposed on oral interception for the purpose of minimizing the intrusion consist-

as well as the application for the surveillance order and supporting materials, could be released to the individuals indicted as a result of the government's investigation.

ently with the requirements of such title. 18 U.S.C.A. § 2518.

MEMORANDUM

KEETON, District Judge.

The United States has applied for an order authorizing interception of oral communications in accordance with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510 *et seq.*, and for simultaneous videotape surveillance. The application seeks authorization for surreptitious entry into a private dwelling and implantation of monitoring devices within the dwelling, subject to the limitations of the proposed authorization.

The proposed surveillance is extraordinarily intrusive. The supporting affidavits, however, present compelling evidence of probable cause to believe that ongoing criminal activities, violations of Title 21 of the United States Code, are occurring within the dwelling, that each of the occupants of the dwelling participates in these criminal activities, that investigative procedures thus far used have been without substantial success and that, unless video surveillance as well as oral interception is used, available alternative investigative procedures are unlikely to succeed in identifying particular participants in these activities and evidencing the extent and nature of their participation. These circumstances present an issue, unresolved in statutes and precedents, as to whether the court may properly authorize video surveillance as well as oral interception.

Title III, providing in stated circumstances for "interception" of "oral communication," 18 U.S.C. § 2518, makes no explicit reference to video surveillance. The government argues that authority for video surveillance is derived from two sources, separately or in combination: (1) the Fourth Amendment to the U.S. Constitution and Fed.R.Crim.P. 41 and 57(b) and (2) the court's inherent authority under the All Writs Act, 28 U.S.C. § 1651, in aid of its jurisdiction founded in Title III of the Omnibus Crime Control and Safe Streets Act

of 1968, as amended. In substance, if not explicitly, the government contends that it need not comply with the strict conditions that Title III imposes in relation to applications for a court order authorizing oral interception.

Title III, 18 U.S.C. § 2510 *et seq.*, repeatedly refers to "interception" of "oral communications" and nowhere explicitly addresses video surveillance. Thus, a candid reading of the statute discloses that Congress did not consider and answer questions regarding video surveillance. This gap—this absence of any mandate in the statute as to video surveillance—apparently extends to the legislative history as well; counsel for the Government has not called the court's attention to, nor has the court found, any reference in the legislative history to video surveillance.

[1] Given that neither the statute nor the legislative history addresses issues regarding video surveillance, the views that might be urged upon a court fall into three general categories: (1) the absence of any provisions in Title III regarding video surveillance implies that no strictures like those of Title III are to be imposed, and the court may authorize video surveillance as long as it is not forbidden by the Fourth Amendment, the Rules of Criminal Procedure, and precedents; (2) the absence of provisions in Title III for video surveillance implies that video surveillance is forbidden; (3) the absence of any provisions in Title III regarding video surveillance leaves all questions about video surveillance unanswered by Title III, with the consequence that courts must of necessity fashion answers to all such questions in light of whatever guidance is available in the constitution, in laws, and in judicial decisions. The first and second of these three approaches give little if any weight to the concern that Congress manifested, in enacting Title III, that investigative methods be chosen with due regard both for investigating effectively and for safeguarding individual rights. The third is the more appropriate approach to questions that are unanswered both in the statute

WHITTAKER v. RAMSEY

423

Cite as 513 F.Supp. 423 (1980)

and in the legislative history. When Congress has not directly addressed and answered a question, courts—including lower courts, until the Supreme Court has spoken—in answering, by necessity, should nevertheless be guided by the aims, principles and policies that manifestly underlie enacted statutes. *Cf. Universal Camera Corp. v. NLRB*, 340 U.S. 474, 487, 71 S.Ct. 456, 463, 464, 95 L.Ed. 456 (1951) (Frankfurter, J.); *Mailhot v. Travelers Insurance Co.*, 375 Mass. 342, 377 N.E.2d 681, 684 (1978).

It seems clear that when Title III of the Omnibus Crime Control and Safe Streets Act of 1968 was under consideration by Congress, "interception" of "oral communications" was the most intrusive form of investigation under scrutiny. Video surveillance, then less well known and less used, has become increasingly significant during intervening years. Most observers would regard it, standing alone, as even more intrusive than interception of oral communications. Clearly, the combination of oral interception and video surveillance is more intrusive than oral interception alone. In these circumstances, judicial deference to aims, policies and principles manifestly underlying Title III's strictures in relation to interception of oral communications should lead to strictures no less severe in relation to video surveillance.

[2] When the Government's pending application was first presented, the court expressed concern that the authorization for this application from the Attorney General's designate, in compliance with Title III, referred only to "interception" of "oral communications" even though the application sought an order for video surveillance as well. The application is now supported by an authorization from a designate of the Attorney General to seek approval of video surveillance as well. The person so acting for the Attorney General, however, is not the same one who authorized the application for oral interception and is not shown to be one designated by the Attorney General to authorize applications for oral interception. In form, the authorizations would

have made a stronger case for the order if a single authorization had been issued by a person duly designated by the Attorney General to approve Title III applications. The court concludes, however, that Title III is not formally applicable to video surveillance and that in the present case substantive safeguards at least as rigorous as those required by Title III, and perhaps more so, have been observed. Moreover, the application represents that the agents implementing the video surveillance will be directed that the video surveillance component be turned on *after* it has been determined from the audio component that communications involving illegal activities or illegal activity itself, within the scope of the proposed investigation, is taking place and that the video component remain on only as long as and under the same constraints as are imposed on oral interception for the purpose of minimizing the intrusion consistently with the requirements of Title III.

In these distinctive circumstances and with these special provisions for minimizing intrusion, the application will be allowed and the proposed order will be entered.



Gerald David WHITTAKER, Petitioner,

v.

Charles "Buck" RAMSEY et al., Respondents.

Civ. No. 4-80-32.

United States District Court,
E. D. Tennessee,
Winchester Division.

Sept. 15, 1980.

County jail prisoner filed petition for writ of habeas corpus. The District Court, Neese, J., held that, even if petitioner waived his right to extradition hearing only

In the
United States Court of Appeals
For the Seventh Circuit

No. 84-1077

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

ALEJANDRINA TORRES, et al.,

Defendants-Appellees.

Appeal from the United States District Court
for the Northern District of Illinois, Eastern Division.
No. 83 CR 494—George N. Leighton, *Judge.*

ARGUED JUNE 8, 1984—DECIDED DECEMBER 19, 1984

Before CUMMINGS, *Chief Judge*, CUDAHY and POSNER,
Circuit Judges.

POSNER, *Circuit Judge.* This appeal by the United States raises two novel and important questions: whether the federal government may ever secretly televise the interior of a private building as part of a criminal investigation and use the videotapes in a criminal trial, and if so whether the warrants under which television surveillance was conducted in this case complied with constitutional requirements. A federal grand jury indicted the four defendants, who are members of the FALN (Fuerzas Armadas de Liberacion Nacional Puertorriquena), on charges of seditious conspiracy (18 U.S.C. § 2384) and related weapons and explosives violations. On the eve of trial, the district judge ordered the suppression of videotapes that the FBI had made as part of its

surveillance of two FALN safe houses. 583 F. Supp. 86, 99-105 (N.D. Ill. 1984). The government appeals this order under 18 U.S.C. § 3731. The videotapes had no sound track; but at the same time that the FBI was televising the interior of the safe houses it was recording the sounds on different equipment. The judge refused to order suppression of the sound tapes, and they are not in issue in this appeal.

The FALN is a secret organization of Puerto Rican separatists that has been trying to win independence for Puerto Rico by tactics that include bombing buildings in New York, Chicago, and Washington. The bombs are assembled and stored, and members of the organization meet, in safe houses rented under false names. The bombings have killed several people, injured many others, and caused millions of dollars of property damage. See 583 F. Supp. at 91; *In re Special February 1975 Grand Jury*, 565 F.2d 407, 409-10 (7th Cir. 1977); *United States v. Rosado*, 728 F.2d 89, 91-92 (2d Cir. 1984); *In re Archuleta*, 561 F.2d 1059, 1060 (2d Cir. 1977); *In re Cueto*, 443 F. Supp. 857, 858 (S.D.N.Y. 1978); Breasted, *3-Year Inquiry Threads Together Evidence on F.A.L.N. Terrorism*, N.Y. Times, April 17, 1977, at p. 1; Donner, *The Age of Surveillance* 459 (1980) (the FALN "is notorious for its unique indifference to personal injury and possible death randomly inflicted by bombs planted in public places"); Motley, *US Strategy to Counter Domestic Political Terrorism* 18, 76 (1983).

The background to the present case is the arrest in 1980 in a Chicago suburb of several members of the FALN, one of whom agreed to help the FBI's investigation of the organization. He identified as members two of the people later charged in this case. FBI agents followed one, who unwittingly led the agents to an apartment in Chicago that was being used as an FALN safe house. The U.S. Attorney obtained from Chief Judge McGarr of the Northern District of Illinois an order authorizing the FBI to make surreptitious entries into the apartment to install electronic "bugs" and television cameras in every room.

The FBI wanted to see as well as hear because it had reason to believe that the people using the safe houses, concerned they might be bugged, would play the radio loudly when they were speaking to each other and also would speak in code, and that the actual assembly of bombs would be carried on in silence. The television surveillance of the first apartment paid off: the FBI televised two of the defendants assembling bombs. On the basis of these observations the FBI obtained a search warrant for the apartment and found dynamite, blasting caps, guns, and maps showing the location of prisons. Tailing the same two defendants led to the second safe house involved in this appeal. Again a warrant was obtained to conduct electronic, including television, surveillance; and it was by televising meetings in this safe house that the other two defendants in this case were identified.

The trial judge held that there was no statutory or other basis for Chief Judge McGarr's order authorizing television surveillance of the safe houses and that therefore the fruits of the surveillance, including the videotapes, would be inadmissible in the defendants' forthcoming trial. 583 F. Supp. at 105. The defendants and amici curiae advance the following additional grounds for this result: television surveillance in criminal investigations (other than of foreign agents) is forbidden by federal statute; it is in any event so intrusive—so reminiscent of the "telescreens" by which "Big Brother" in George Orwell's *1984* maintained visual surveillance of the entire population of "Oceania," the miserable country depicted in that anti-utopian novel—that it can in no circumstances be authorized (least of all, one imagines, in the year 1984) without violating both the Fourth Amendment and the Fifth Amendment's due process clause; and even if all this is wrong, still the particular orders ("warrants," as we shall call them) in this case did not satisfy the requirements of the Fourth Amendment's warrant clause.

The trial judge appears, however, to have overlooked *United States v. New York Tel. Co.*, 434 U.S. 159, 168-70 (1977), where the Supreme Court held that Rule 41 of the Federal Rules of Criminal Procedure, which authorizes the issuance of search warrants, embraces orders to install "pen registers" (devices that record the phone numbers that a telephone subscriber is dialing). See also *Michigan Bell Tel. Co. v. United States*, 565 F.2d 385, 388-89 (6th Cir. 1977); *United States v. Hall*, 583 F. Supp. 717, 718-19 (E.D. Va. 1984). Although the language of Rule 41 is that of conventional searches (see especially subsection (b)), the Court in the *New York Telephone* case read the rule flexibly and concluded that it covers "electronic intrusions" as well—including bugging. 434 U.S. at 169 (dictum). We cannot think of any basis on which the rule might be thought sufficiently flexible to authorize a pen register, bug, or wiretap, but not a camera. It is true that secretly televising people (or taking still or moving pictures of them) while they are in what they think is a private place is an even greater intrusion on privacy than secretly recording their conversations. But the fact that electronic eavesdropping is more intrusive than conventional searching did not prevent the Supreme Court in the *New York Telephone* case from reading Rule 41—very broadly in view of its language—to embrace electronic eavesdropping. The next step, to television surveillance, is smaller than the one the Court took.

There is another basis, besides Rule 41, for the issuance of warrants for television surveillance. Like the power to prescribe or regulate procedure, to punish for contempts of court, and to issue writs in aid of the court's jurisdiction, the power to issue a search warrant was historically, and is still today, an inherent (by which we mean simply a nonstatutory, or common law) power of a court of general jurisdiction. Indeed, it is an aspect of the court's power to regulate procedure. A search warrant is often used to obtain evidence for use in a criminal proceeding, and is thus a form of (or at least an analogue to) pretrial discovery. Although Congress can limit the

procedural authority of the federal courts—if nothing else, Congress's power to create lower federal courts (Art. I, § 8, cl. 9) so implies—until it does so with respect to a particular subject the courts retain their traditional powers. Rule 57(b) of the Federal Rules of Criminal Procedure virtually so states. And much of federal criminal procedure, especially in the early days of the federal courts, was judge-made. Orfield, *Early Federal Criminal Procedure*, 7 Wayne L. Rev. 503 (1961), gives a number of examples, though none involve search warrants. See *id.* at 529.

In England the inherent judicial power to issue warrants (warrants to seize persons and things and therefore implicitly to search for them) goes back very far—perhaps to the twelfth century. See Baker, *An Introduction to English Legal History* 15 (2d ed. 1979); *Crown Pleas of the Wiltshire Eyre, 1249*, at 75, 92, 98, 100 (Meekings ed. 1961). By the seventeenth century the power was firmly lodged in the justices of the peace. See Dalton, *The Countrey Justice 1619*, at 300-06 (1972 reprint ed. [1622]); Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* 36 n. 86 (1937). Hale's *History of the Pleas of the Crown* (1736) makes clear that the justices of the peace could issue search warrants, provided they were not general warrants. See passages quoted in Scarborough & White, *Constitutional Criminal Procedure* 21 (1977). As the justices of the peace were not even lawyers, it seems likely that the judges of the royal courts (from which many features of the federal courts were borrowed) had the same power, if little or no occasion to exercise it. A modern American parallel is Rule 41(a) of the Federal Rules of Criminal Procedure, which in terms authorizes only federal magistrates and state-court judges to issue search warrants (see 3 Wright, *Federal Practice and Procedure: Criminal* 2d, pp. 571-73 nn. 1-7 (1982)) but has been uniformly assumed (for example in the *New York Telephone* case) to empower federal district judges as well to issue search warrants.

Although *Entick v. Carrington*, 19 Howell's State Trials 1029 (C.P. 1765), has been cited for the proposition that statutory authority was required in England for the issuance of search warrants, see, e.g., *United States v. Finazzo*, 583 F.2d 837, 843 (6th Cir. 1978), summarily vacated on other grounds, 441 U.S. 929 (1979), the only issue in *Entick* was whether a nonjudicial officer (the secretary of state, described in the opinion as "the king's private secretary," 19 Howell's State Trials at 1046) had common law authority to issue a general warrant to investigate seditious libel. See *id.* at 1063-74. The court held he did not, but did not express doubt about the power of judicial officers to issue particularized warrants. Cf. *Boyd v. United States*, 116 U.S. 616, 629-30 (1886); Lasson, *supra.* at 47-49; cf. *id.* at 34-37, 51-78; Dickerson, *Writs of Assistance as a Cause of the Revolution*, in *The Era of the Revolution* 40, 75 (Morris ed. 1939).

The power to issue a search warrant is a common law power in America as well as England, see *Adams v. New York*, 192 U.S. 585, 598 (1904); *Boyd v. United States*, *supra.* 116 U.S. at 623; *United States v. Maresca*, 266 Fed. 713, 721 (S.D.N.Y. 1920) (Hough, J.), and in the federal system as well as in the states. While "the whole criminal jurisdiction of the courts of the United States [is] derived from Acts of Congress," *Jones v. United States*, 137 U.S. 202, 211 (1890), this does not mean that every procedural incident of their jurisdiction is statutory. Until 1917 there was no general statutory authorization for the issuance of federal search warrants; yet it is hard to believe that before then no warrants were issued outside of the few specific areas (discussed in *United States v. Jones*, 230 Fed. 262, 265-68 (N.D.N.Y. 1916)) in which Congress had explicitly authorized their issuance, usually by United States Commissioners. So we are not surprised to have found cases which assume as if it were an uncontroversial proposition that federal courts could issue such warrants before 1917. See *Weeks v. United States*, 232 U.S. 383 (1914); *In re Jackson*, 96 U.S. 727, 733 (1878); *Agnello v. United States*, 290 Fed. 671, 677 (2d Cir. 1923); but cf.

United States v. Jones, supra, 230 Fed. at 268. We are only surprised not to have found more such cases.

In 1917 Congress enacted as part of the Espionage Act its first and last general authorization to federal courts to issue search warrants. See 40 Stat. 228-230, 18 U.S.C. §§ 611-633 (1940 ed.). Judging from the committee reports, Congress seems not to have thought it was granting the courts a new power as distinct from creating a procedural framework for the exercise of an old one, cf. H.R. Conf. Rep. No. 65, 65th Cong., 1st Sess. 20 (1917); H.R. Conf. Rep. No. 69, 65th Cong., 1st Sess. 20 (1917), although the floor debates indicate that a number of Congressmen—and the Attorney General of the United States—thought that without the new statute the federal courts would be helpless to authorize search warrants outside of the specific areas covered by previous statutes authorizing search warrants. See 55 Cong. Rec. 1838-39, 2065 (1917).

When Congress overhauled the federal criminal code in 1948, it repealed most of the search-warrant provisions of the Espionage Act, see Notes of Advisory Committee on Fed. R. Crim. Proc. 41, thereby leaving the matter of search warrants to be governed by rule of court. This broad delegation suggests that Congress views the issuance of federal search warrants as standing on a plane with other procedural powers that courts traditionally have exercised without explicit legislative direction. Additional evidence of this is found in the electronic-eavesdropping cases decided by the Supreme Court before the enactment in 1968 of Title III (of which more shortly), which explicitly authorized warrants for electronic eavesdropping. *Osborn v. United States*, 385 U.S. 323, 328-31 (1966), upheld without mention of Rule 41 a federal court order authorizing a police officer to carry a concealed recording device, and *Katz v. United States*, 389 U.S. 347, 354-56 (1967), stated that a federal warrant could authorize bugging, and made only a passing reference to Rule 41(d) (execution and return). See *id.* at 355 n. 16. Other authorities for the inherent power of the federal courts to

issue search warrants include *United States v. Williams*, 617 F.2d 1063, 1099 (5th Cir. 1980) (en banc) (concurring opinion), and *United States v. Yuck Kee*, 281 Fed. 228, 230-31 (D. Minn. 1922); see also *United States v. Cafero*, 473 F.2d 489, 499 (3d Cir. 1973).

We shall not pretend greater certainty than we feel that the federal courts can authorize new types of search without statutory authorization, though *New York Telephone* is powerful authority. The historical evidence we have marshaled is, as so commonly is the case, incomplete and enigmatic; and the floor debates on the 1917 search-warrant provisions are contrary to our position, as is Congress's quick passage of a statute to permit searches for "mere evidence" after the Supreme Court held that the Fourth Amendment did not forbid such searches. See 18 U.S.C. § 3103a; 3 Wright, *supra*, § 664, at pp. 607-08. But a conclusion that neither Rule 41 nor the inherent common law powers of the federal courts allow warrants for television surveillance would have a most curious implication that in combination with all else we have said persuades us to reject it. A search without a warrant certainly is permissible in an emergency, see, e.g., *Welsh v. Wisconsin*, 104 S. Ct. 2091, 2097 (1984); *Warden v. Hayden*, 387 U.S. 294, 297-99 (1967); and a situation in which the FBI had strong reason to believe that an organization was operating a bomb factory but the FBI could not obtain a warrant to conduct the only type of search that would be effective in obtaining necessary evidence of this, because no court had been given authority to issue such a warrant, could fairly be described as an emergency. Therefore the government would have an argument that the fruits of such a search, though it had been conducted without a warrant, would be admissible in the criminal proceeding, provided the search was otherwise reasonable (an important qualification, as we shall see). A holding that federal courts have no power to issue warrants authorizing television surveillance might, therefore, simply validate the conducting of such surveillance without warrants. This would be a Pyrrhic victory for those who view the search

warrant as a protection of the values in the Fourth Amendment.

The defendants argue, however, that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2520, as amended by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801 *et seq.*, deprives the federal courts of the power they would otherwise have to issue a warrant for television surveillance. Title III authorizes federal judges to issue warrants (called "orders") for wiretapping and bugging, and establishes elaborate requirements for such warrants. See 18 U.S.C. §§ 2516, 2518. But it does not authorize warrants for television surveillance. *People v. Teicher*, 52 N.Y.2d 638, 652, 422 N.E.2d 506, 513 (1981); *Sponick v. City of Detroit Police Dep't*, 49 Mich. App. 162, 198, 211 N.W.2d 674, 690 (1973); Carr, *The Law of Electronic Surveillance* 124 (1977). The statute regulates only the "interception of wire or oral communications." 18 U.S.C. §§ 2516(1), 2518(1); see also 18 U.S.C. §§ 2511-2513, 2515, 2517, 2519. A man televised while silently making a bomb is not engaged in any form of communication, let alone "wire or oral communication." Any possible doubt on this score is dispelled by the statutory definition of "intercept" as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). A visual observation is in no possible sense an "aural acquisition," or an acquisition, of any kind, of a "wire or oral communication." Nor would a camera meet the statutory definition of "electronic, mechanical, or other device." See 18 U.S.C. § 2510(5). The Senate committee report, after repeating the statutory definition of "aural acquisition," remarks: "Other forms of surveillance are not within the proposed legislation." S. Rep. No. 1097, 90th Cong., 2d Sess. 90 (1968).

It does not follow, however, that because Title III does not authorize warrants for television surveillance, it forbids them. The motto of the Prussian state—that everything which is not permitted is forbidden—is not a helpful

guide to statutory interpretation. Television surveillance (with no soundtrack) just is not within the statute's domain. The legislative history does not refer to it, probably because television cameras in 1968 were too bulky and noisy to be installed and operated surreptitiously. It would be illogical to infer from Congress's quite natural omission to deal with a nonproblem that it meant to tie the federal courts' hands when and if the problem arose.

The defendants appeal to the spirit of Title III, which was, they say, the protection of privacy, and from which they infer that Congress meant to forbid any electronic investigative techniques that it did not authorize. But this description of the spirit of Title III is incomplete. Enacted in the wake of *Katz v. United States, supra*, which had held that electronic eavesdropping was subject to the Fourth Amendment, Title III established procedures to facilitate the use of wiretapping and bugging (subject to appropriate safeguards) in federal criminal investigations. Protecting privacy was a goal of the statute but not the only or even the paramount goal. The Senate report states that "Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." S. Rep. No. 1097, 90th Cong., 2d Sess. 66 (1968). The second formulation seems an allusion to the law-enforcement objectives of Title III, elsewhere in the report described as paramount. "[T]he major purpose of title III is to combat organized crime"; and "intercepting the communications of organized criminals is the only effective method of learning about their activities." *Id.* at 70, 72.

The Foreign Intelligence Surveillance Act establishes procedures for electronic surveillance of foreign agents. Reflecting changes in technology in the decade that had passed since the enactment of Title III, the Act defines electronic surveillance broadly enough to cover television, by including in the definition the use of "an electronic, mechanical, or other surveillance device . . . for monitoring

No. 84-1077

11

to acquire information, other than from a wire or radio communication" 50 U.S.C. § 1801(f)(4); see S. Rep. No. 604, 95th Cong., 2d Sess., pt. 1, at 35 (1977). Although the procedures in the Act have no direct application to this case—these defendants are not agents of a foreign power, and the government does not argue that the Act authorized television surveillance of them—the Act also amended Title III as follows: "procedures in [Title III] and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined [in the Foreign Intelligence Surveillance Act], and the interception of domestic wire and oral communications may be conducted." 18 U.S.C. § 2511(2)(f). The defendants read this to mean that television surveillance, a form of electronic surveillance that does not involve the interception of wire or oral communications, may be conducted only in accordance with the Foreign Intelligence Surveillance Act; since that Act did not authorize the surveillance in this case, section 2511(2)(f) forbids it.

All this section means to us, however, is that the Foreign Intelligence Surveillance Act is intended to be exclusive in its domain and Title III in its. The powers that the Act gives the government to keep tabs on agents of foreign countries are not to be used for purely domestic investigations, and conversely the limitations that Title III places on wiretapping and bugging are not to be used to hobble the government's activities against foreign agents. To read the Foreign Intelligence Surveillance Act as the defendants would have us do would give a statute designed to regularize the government's broad powers to deal with the special menace posed by agents of foreign powers the side effect of curtailing the government's powers in domestic law enforcement. This is not what Congress intended in making what the Senate report on the bill that became the Foreign Intelligence Surveillance Act described as a "technical and conforming" amendment to Title III. S. Rep. No. 604, *supra*, at 3.

It is true that the committee reports describe section 2511(2)(f) as the "exclusive congressional statement on the question of the Executive's power to order electronic surveillance," *id.* at 63; see also S. Rep. No. 701, 95th Cong., 2d Sess. 71-72 (1978); H.R. Conf. Rep. No. 1720, 95th Cong., 2d Sess. 35 (1978); and on this language can be built an argument that Congress intended in section 2511(2)(f) to take away not only the power the courts would otherwise have under Rule 41 or common law principles to issue warrants for television surveillance outside the scope of the Foreign Intelligence Surveillance Act, but also the President's implicit power, deriving from Article II of the Constitution, to use television surveillance for the protection of national security, other than as permitted by that Act. But the background of the quoted language makes this a weak argument. The Foreign Intelligence Surveillance Act is about national security; and much concern was expressed in the debates about the constitutionality as well as the prudence of Congress's displacing by legislation the President's implicit authority under Article II to protect the nation's security against intrigues by foreign powers. See, e.g., 124 Cong. Rec. 28137 (1978) (remarks of Representative Butler). The debate was resolved in favor of the proposed legislation. But the question whether to curtail executive power in domestic criminal investigations was not on the legislative agenda and so far as we can determine was not intended to be answered by the brief discussion in the committee reports of a "technical and conforming" amendment to Title III.

The fact is that Congress has never addressed the issue of judicial authorization of television surveillance in federal criminal investigations. But of course that observation cannot be the end of our analysis. It is too late in the day to argue that the Fourth Amendment regulates only the types of search that were technically feasible in the eighteenth century. The government therefore quite properly does not argue that television surveillance is outside the scope of the Fourth Amendment. We think it

also unarguable that television surveillance is exceedingly intrusive, especially in combination (as here) with audio surveillance, and inherently indiscriminate, and that it could be grossly abused—to eliminate personal privacy as understood in modern Western nations.

The precise application of the Fourth Amendment to television surveillance has, therefore, now to be considered. The Fourth Amendment provides: “[1] The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and [2] no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” The usual way in which judges interpreting the Fourth Amendment take account of the fact that searches vary in the degree to which they invade personal privacy is by requiring a higher degree of probable cause (to believe that the search will yield incriminating evidence), and by being more insistent that a warrant be obtained if at all feasible, the more intrusive the search is. See, e.g., *Gooding v. United States*, 416 U.S. 430, 464-65 (1974) (dissenting opinion); *United States v. Karo*, 104 S. Ct. 3296, 3304-05 (1984). But maybe in dealing with *so* intrusive a technique as television surveillance, other methods of control as well, such as banning the technique outright from use in the home in connection with minor crimes, will be required, in order to strike a proper balance between public safety and personal privacy. Cf. *United States v. Preston*, 468 F.2d 1007, 1010 (6th Cir. 1972); *Nueslein v. District of Columbia*, 115 F.2d 690, 696 (D.C. Cir. 1940); *Brinegar v. United States*, 338 U.S. 160, 183 (1949) (Jackson, J., dissenting); 1 LaFare & Israel, *Criminal Procedure* § 3.3, at p. 187 (1984). That question is not before us, but we mention it to make clear that in declining to hold television surveillance unconstitutional *per se* we do not suggest that the Constitution must be interpreted to allow it to be used as generally as less intrusive techniques can be used. The first clause of the Fourth Amendment guarantees the right of the

American people to be free from unreasonable searches by federal (and by judicial interpretation of the Fourteenth Amendment, state) officers; and a search could be unreasonable, though conducted pursuant to an otherwise valid warrant, by intruding on personal privacy to an extent disproportionate to the likely benefits from obtaining fuller compliance with the law. "[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." *Camara v. Municipal Court*, 387 U.S. 523, 536-37 (1967).

But we do not think there can never be a case where secretly televising people in private places is reasonable. The facts of the present case argue against so absolute an approach. The FALN has the plans, the materials, and the know-how to kill in gross. A sophisticated as well as lethal practitioner of urban terrorism, it meets to plan its operations and assemble bombs in safe houses leased under false names. Alert to the possibility that its safe houses might be bugged by the FBI, it takes effective steps to defeat this form of electronic surveillance, making it highly resistant to conventional methods of law enforcement even as enhanced by modern techniques for overhearing conversations. We do not think the Fourth Amendment prevents the government from coping with the menace of this organization by installing and operating secret television cameras in the organization's safe houses. The benefits to the public safety are great, and the costs to personal privacy are modest. A safe house is not a home. No one lives in these apartments, amidst the bombs and other paraphernalia of terrorism. They are places dedicated exclusively to illicit business; and though the Fourth Amendment protects business premises as well as homes, e.g., *Marshall v. Barlow's Inc.*, 436 U.S. 307, 311-12 (1978), the invasion of privacy caused by secretly televising the interior of business premises is less than that caused by secretly televising the interior of a home, while the social benefit of the invasion is greater when the organization under investigation runs a bomb factory than it would be if it ran a chop shop or a numbers parlor.

There is no right to be let alone while assembling bombs in safe houses.

Having concluded that the district court could validly authorize television surveillance in this case, we come to the question whether the two warrants complied with the requirements of the Fourth Amendment's warrant clause. On this aspect of the case the defendants do not argue that the warrants were not issued on the basis of an oath and probable cause, but that they are not particular enough to satisfy the requirements of the Fourth Amendment. (They also make two highly technical objections to the warrants, which we shall take up last.)

The government asked for the warrants in its applications for Title III warrants—applications the government had to make because it wanted to record the sounds in the apartments at the same time that it was televising the interiors—and the warrants it got covered both methods of surveillance. Title III imposes many restrictions on intercept warrants. Those related to the constitutional requirement of particularity are that the judge must certify that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," 18 U.S.C. § 2518(3)(c), and that the warrant must contain "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," § 2518(4)(c), must not allow the period of interception to be "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days" (though renewals are possible), § 2518(5), and must require that the interception "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under [Title III]," *id.* Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment's requirement of particular description. Cf. *United States v.*

Terry, 702 F.2d 299, 312 (2d Cir. 1983); Carr, *supra*, § 5.07[1] at p. 256.

After stating that there was probable cause to believe both that the individuals named in the warrant were using the specified premises (the safe house) in connection with specified federal crimes and that intercepts of oral and wire communications at this address would yield evidence concerning these crimes, after stating that normal investigative methods had been tried and had failed, and after authorizing intercepts at the address, each of the original warrants in this case went on to authorize the FBI "to install [at the address] devices that will visually monitor and record the activity taking place in furtherance of the above-described [illegal] purposes." Each warrant then specified the number of surreptitious entries that the FBI was authorized to make to install, adjust, and remove both the audio and video equipment (a total of 34 separate entries were authorized), required progress reports to be made to the court every five days, required that the electronic surveillance cease "upon the attainment of the authorized objective," and put a deadline of 30 days on both the audio and video surveillance. One of the warrants was renewed a total of four times, so that it authorized a total of 150 days of surveillance, and the other was renewed twice; and in all, 130 hours of videotape were made. The renewal warrants were essentially identical to the original ones, but were supported by even more compelling showings of probable cause, based on information yielded by the execution of the original warrants.

In short, the warrants complied with all four of the requirements of Title III that implement the constitutional requirement of particularity. In fact, the only requirement of Title III that the government may not have complied with in its television surveillance was the requirement that the application be authorized by the Attorney General or an Assistant Attorney General specially designated by him. See 18 U.S.C. § 2516(1). Actually, the authorization *was* obtained; it just was not communicated to the district judge. We need not decide

whether this was a failure to comply with the statute, (nothing in the statute suggests it is); it is in any event not relevant to the Fourth Amendment's requirement of particularity.

A warrant for video surveillance that complies with those provisions that Congress put into Title III in order to implement the Fourth Amendment ought to satisfy the Fourth Amendment's requirement of particularity as applied to such surveillance. Title III was Congress's carefully thought out, and constitutionally valid (see, e.g., *United States v. Ramsey*, 503 F.2d 524, 530-31 (7th Cir. 1974); *United States v. Tortorello*, 480 F.2d 764, 772-75 (2d Cir. 1973)), effort to implement the requirements of the Fourth Amendment with regard to the necessarily unconventional type of warrant that is used to authorize electronic eavesdropping. In a conventional search the police go through a home or an office looking for contraband or evidence of a crime, and they either find what they are looking for or not, and then they leave. By rummaging through a person's possessions in search of what they came for they invade the person's privacy, and much of what they examine may be at once personal and irrelevant to the objective of the search, but the search is usually brief. Electronic interception, being by nature a continuing rather than one-shot invasion, is even less discriminating than a physical search, because it picks up private conversations (most of which will usually have nothing to do with any illegal activity) over a long period of time. Whether because it is more indiscriminate, or because people regard their conversations as more private than their possessions, or for both reasons, electronic interception is thought to pose a greater potential threat to personal privacy than physical searches, and Congress therefore pitched the requirements for a valid intercept warrant higher than those for a conventional Rule 41 warrant: except for probable cause, the requirements in 18 U.S.C. § 2518 are not found in Rule 41. Television surveillance is identical in its indiscriminate character to wiretapping and bugging. It is even more invasive of privacy, just as a strip search is

more invasive than a pat-down search, but it is not more indiscriminate: the microphone is as "dumb" as the television camera; both devices pick up anything within their electronic reach, however irrelevant to the investigation. If the government conducts television surveillance in conformity with the requirements of particularity that Title III imposes on electronic eavesdropping (not literal conformity, of course, since words such as "communications" and "intercept" in Title III do not fit television surveillance), the government has also conformed to the requirement of particularity in the Fourth Amendment's warrant clause.

Since the government did this here, we need not, strictly speaking, decide what would happen if it had not done so. But because television surveillance is potentially so menacing to personal privacy, we want to make clear our view that a warrant for television surveillance that did not satisfy the four provisions of Title III that implement the Fourth Amendment's requirement of particularity would violate the Fourth Amendment. Invoking our common law power to interpret the Constitution in a novel context, we borrow the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold that it provides the measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime. We doubt that the government will resist this view, for there will be few if any cases where it does not try anyway to conform its application for a television-surveillance warrant to Title III. It wants the sounds as well as the sights, and it can get a warrant for the former only by complying with Title III; the soundtrack of a videotape, no less than a free-standing tape recording, is within the scope of Title III, as assumed in *United States v. Haimowitz*, 725 F.2d 1161, 1581 and n. 28 (11th Cir. 1984).

But we are unwilling to go further and hold that warrants for television surveillance are subject to Title III, as warrants for bugging and wiretapping are, so that if for example a television-surveillance warrant was de-

stroyed without an order by the issuing judge, the person destroying it could be punished for contempt under 18 U.S.C. § 2518(8)(c), a provision of Title III that punishes unauthorized destruction of intercept warrants. It is only the requirements (listed earlier) of Title III that implement the constitutional requirement of particularity in the novel setting of electronic surveillance that we have borrowed to give content to the Fourth Amendment as applied to television surveillance. Of course it is anomalous to have detailed statutory regulation of bugging and wiretapping but not of television surveillance, in Title III, and detailed statutory regulation of television surveillance of foreign agents but not of domestic criminal suspects, in the Foreign Intelligence Surveillance Act; and we would think it a very good thing if Congress responded to the issues discussed in this opinion by amending Title III to bring television surveillance within its scope. But judges are not authorized to amend statutes even to bring them up to date. True, when statutes are ambiguous and judges interpret them in light of altered conditions, the result is very like amendment. "When a judge tries to find out what the government would have intended which it did not say, he puts into its mouth things which he thinks it ought to have said, and that is very close to substituting what he himself thinks right. Let him beware, however, or he will usurp the office of government, even though in a small way he must do so in order to execute its real commands at all." L. Hand, *How Far Is a Judge Free in Rendering a Decision?*, in *The Spirit of Liberty* 103, 108 (Dilliard 3d ed. 1960 [1935]). Judge Hand's warning about judicial usurpation is apt here. When Congress has indicated the domain of a statute as clearly as it did when it enacted Title III, we cannot apply the statute outside its domain merely because we are confident that if Congress had known then what we know now it would have used more general language. Congress said in language that could not be clearer that Title III is about the interception of wire and oral *communications* and that interception means *aural* acquisition. There is no way in which these

words can be read to include silent television surveillance; and the legislative history quoted earlier indicates that the exclusion from the scope of the statute of other methods of surveillance besides those defined in the statute was deliberate. Statutory language, to be stretchable, should be elastic. This statutory language is not. To read the words of this statute—intercept, aural, communication—as if they encompassed silent visual surveillance would be to say to Congress that there is no form of words that it can use to mark off the limits of a statute that will prevent aggressive, imaginative judges from disregarding those limits. And we naturally shrink from saying any such thing.

If Title III and the Foreign Intelligence Surveillance Act were inconsistent, then we would have to make a choice, and in doing so we might unavoidably be exercising something resembling a legislature's discretion. But there is no inconsistency. The two statutes govern nonoverlapping domains. And television surveillance for domestic criminal investigations is in neither statute's domain. No doubt this is, as we have said, anomalous; it may seem fairly to cry out for congressional attention; but it does not create ambiguity as to the legal duties under which the government labors in conducting television surveillance of domestic criminal suspects. The only legal duties are those imposed by the Fourth Amendment. And we therefore go as far as is proper for us to go when we use a part of Title III to give meaning to the Fourth Amendment's requirement of particularity as applied to television surveillance. Since the Fourth Amendment has long been held fully applicable to the states through the Fourteenth Amendment, state and local officers who might want to use television surveillance in criminal investigations will be under the same restraints as we impose on federal officers today.

The defendants complain, finally, that the warrants in this case did not explain the basis of the judge's finding of probable cause and did not identify as safe houses the addresses at which the surveillance was to be conducted. This complaint misapprehends the purpose of a search

warrant, which is twofold: to show that a judicial officer authorized the search (cf. *Johnson v. United States*, 333 U.S. 10, 13-14 (1948)), and to indicate to the government agents who will execute the warrant what the limits of the authorization are (cf. *Marron v. United States*, 275 U.S. 192, 196 (1927)). A warrant is not a judicial opinion, and the basis for the warrant is not in the warrant itself; as Rule 41(c)(1) makes clear, it is in the application for the warrant. The application in this case set forth in full and convincing detail the reasons for thinking that the addresses where the surveillance was to be conducted were FALN safe houses, that normal investigative methods would be unavailing, and that television surveillance was an appropriate supplement to electronic eavesdropping. The truth of the recitals in the applications is not controverted, and they provided an adequate factual basis for the warrants.

The order of suppression is reversed and the case remanded for trial.

REVERSED AND REMANDED.

CUDAHY, *Circuit Judge*, concurring in the result. I am in complete accord with the majority's conclusion that "[t]here is no right to be let alone while assembling bombs in safe houses." It is hard to imagine facts stronger than those before us to justify means of surveillance necessary to protect the public. No society may be lightly presumed to have denied itself the means necessary to defend itself against this kind of assault.

If there were no Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197, 212, codified primarily as chapter 119 of 18 U.S.C., and no Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. 95-511, 92 Stat. 1783, codified primarily as chapter 36 of 50 U.S.C., I would have no great difficulty in this case in following the majority down the

path of inherent powers (fortified by Rule 41 of the Federal Rules of Criminal Procedure). That route has considerable appeal where, as here, we are apparently responding to the threat of a war to be waged randomly against the populace. But given the existing statutory scheme, that route is, I think, neither necessary nor justifiable.

I believe that, if Title III and FISA are construed together, it is possible and desirable to find in them not only the authority to conduct video surveillance in appropriate circumstances but a procedure which brings authorization of, and responsibility for, such surveillance under centralized and high-level control. Considering the potential of video surveillance to lend dreadful substance to the Orwellian concerns noted by the majority, we should be extremely reluctant to permit this sort of activity free of the statutory safeguards provided by Congress for less intrusive police activities. And it is not as difficult, apparently, for me to find a basis for application of the safeguards of Title III and FISA as it is for the majority. In that connection, it is worth repeating that while

[i]t is not the judge's job to keep a statute up to date in the sense of making it reflect contemporary values[,] it is his job to imagine as best he can how the legislators who enacted the statute would have wanted it applied to situations they did not foresee.

Posner, *Statutory Interpretation—in the Classroom and in the Courtroom*, 50 U. CHI. L. REV. 800, 818 (1983). This court itself has recently recognized that

[t]he judicial duty of statutory interpretation is not a duty merely to read; it is a duty to help the legislature achieve the aims that can reasonably be inferred from the statutory design, and it requires us to pay attention to the spirit as well as the letter of the statute.

United States v. Markgraf, 736 F.2d 1179, 1188 (7th Cir. 1984) (Posner, J., dissenting from denial of rehearing *en banc*). If these injunctions require one to be—in the

words of the majority—"aggressive" and "imaginative," then so be it.

In my view, a careful evaluation of Title III and FISA, and of the interplay between those two statutes, shows that the video surveillance in this case should be subject to the requirements of Title III. Neither party now advocates this position, but it appears to have been the government's position when it sought the court orders here and it was Judge McGarr's approach when he issued the orders.¹

The foundation of my position is that Title III must be construed together with FISA, and that it is clear that Congress intended the statutes to be read together, providing a comprehensive and exclusive system of control. See S. REP. NO. 604, 95th Cong., 1st Sess. 3, 6, 15, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3904, 3907, 3916-17 (Judiciary Comm.); *see also* S. REP. NO. 701, 95th Cong., 2d Sess. 71, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 4040 (Intelligence Comm.). The two statutes are written to impose a comprehensive regulatory scheme on the use of electronic surveillance in the United States whenever there is a reasonable expectation of privacy. Title III was enacted to govern domestic surveillance activity, and as enacted in 1968 it expressly exempted from its provisions electronic surveillance for national security purposes. Section 802, Pub. L. 90-351, 82 Stat. 197, 213, *codified as* 18 U.S.C. § 2511(3), *repealed by* § 201(c) of FISA. In 1978, Congress responded to concerns about the abuse of that national security exemption by enacting FISA. S. REP. NO. 604, 95th Cong., 1st Sess. 7, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3908. FISA repealed the exemption and declared that the executive branch does not have inherent authority to undertake electronic surveillance even in national security and

¹ See Initial Buena Application at 6, Gov't App. at 101; Initial Lunt Application at 5, Gov't App. at 232; Transcript of Initial Buena Application-Order Proceedings before Judge McGarr, January 18, 1983, at 2-3, Gov't App. at 223-24.

counterintelligence cases. S. REP. NO. 604, 95th Cong., 1st Sess. 6, 64, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3907, 3965, S. REP. NO. 701, 95th Cong., 2d Sess. 71, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 4040. Instead, FISA created a new set of procedures and substantive requirements which would subject such surveillance to judicial control while still protecting national security. Several provisions of FISA make it unmistakably clear that government (federal, state and local) may not use highly intrusive forms of electronic surveillance unless it does so in accordance with either Title III or FISA. *E.g.* 18 U.S.C. § 2511(2)(f) (codifying § 201(b) of FISA); 50 U.S.C. § 1809 (codifying § 109 of FISA). Unless those statutes are complied with, law enforcement officers who engage in these forms of surveillance may very well be committing a federal crime. 50 U.S.C. § 1809.

The basic problem in the case before us stems from the fact that FISA explicitly addresses the problem of video surveillance, while Title III does not. The majority errs in concluding that the government may engage in the video surveillance in this case without regard to any statutory regulation of such surveillance. In doing so, the majority ignores unequivocal provisions of FISA, and of Title III as amended by FISA, and disregards the clear purpose of both statutes to subject intrusive forms of electronic surveillance to strict statutory control.

The key statutory provisions here are 18 U.S.C. § 2511(2)(f), enacted as section 201(b) of FISA, and 50 U.S.C. § 1809, enacted as section 109 of FISA. Section 2511(2)(f) of title 18, U.S.C., provides in relevant part:

[P]rocedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 *shall be the exclusive means* by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted. (emphasis supplied)

This provision incorporates the FISA definition of "electronic surveillance" found in 50 U.S.C. § 1801(f).

Subparagraph 4 of that subsection defines "electronic surveillance" as

the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

That language is obviously broad, and, read literally, certainly includes video surveillance. There is no doubt that the miniaturized cameras used in this case are "electronic devices" used "to acquire information" under circumstances in which the subjects had a reasonable expectation of privacy. And when we turn to the relevant committee reports on FISA, we learn that Congress did in fact intend the quoted language to cover such video surveillance equipment. S. REP. NO. 604, 95th Cong., 1st Sess. 35, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3936; S. REP. NO. 701, 95th Cong. 2d Sess. 37, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 4006. The Senate Judiciary Committee Report on FISA explains that that subparagraph "could also include miniaturized television cameras and other sophisticated devices not aimed merely at communications." S. REP. NO. 604, 95th Cong., 1st Sess. 35, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3936. The next sentence of the report says "[t]his part of the definition is meant to be broadly inclusive, because the effect of including a particular means of surveillance is not to prohibit it but to subject it to judicial oversight." *Id.* The Senate Intelligence Committee Report on the bill includes the same language. See S. REP. NO. 701, 95th Cong., 2d Sess. 37, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 4006.

Thus, it is clear that video surveillance falls within the FISA definition of electronic surveillance. Therefore, 18 U.S.C. § 2511(2)(f) may be paraphrased to say that the

"procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance—including video surveillance—may be conducted." In short, if the video surveillance employed in this case was not expressly authorized by either Title III or FISA, then it would be prohibited by law. Subsection 2511 (2)(f) cannot be contorted into meaning that Title III governs one thing, FISA governs another, and anything not governed by one or the other is permitted, as the majority would have it.

In addition, if the video surveillance here was not authorized by statute, then the officers who engaged in it may have committed a federal crime. Section 109(a) of FISA, 50 U.S.C. § 1809(a), provides in relevant part: "A person is guilty of an offense if he intentionally—(1) engages in electronic surveillance under color of law except as authorized by statute" Again, the FISA definition of "electronic surveillance" applies to this provision, and as shown above, that definition includes video surveillance such as that used in the case before us.² Section 1809 thus requires the government to show *statutory* authorization for its use of video surveillance, and the only possible sources of that authority are Title III and FISA.

But my reasons for disagreeing with the majority are not limited to the statutory language. By leaving an extraordinarily intrusive form of domestic electronic surveillance uncontrolled by statute, the majority acts contrary to the purposes of both statutes and produces a highly improbable result.

² Of course, subsection (b) of the section (50 U.S.C. § 1809(b)) provides a defense for officers with a search warrant or court order, so the officers in the matter before us presumably would not be in jeopardy. By finding that courts have the power to issue warrants for video surveillance, even though not authorized by statute, the majority effectively eviscerates this criminalizing provision.

This most improbable result may be described in the following way. Based on the definition of "electronic surveillance" in FISA, 50 U.S.C. § 1801(f)(4), any attempt to employ video surveillance in a foreign intelligence case would be subject to FISA's restrictions. In these highly sensitive cases of perhaps extraordinary importance to the nation, video surveillance may be employed only with the approval of officials at the highest levels of the federal government and of a special court established for this purpose in 50 U.S.C. § 1803. To be more precise, the application must be approved by the Attorney General or Deputy Attorney General of the United States, 50 U.S.C. § 1804(a); and the need for using such intrusive surveillance measures must be certified by the President's national security affairs adviser or a national security official whose appointment is subject to Senate confirmation, 50 U.S.C. § 1804(a)(7). Only then may the government apply to the special court for a warrant. And FISA imposes numerous other requirements designed to ensure that highly intrusive surveillance measures are used only when and to the extent necessary. See the remainder of § 1804(a).

In sharp contrast to these extraordinary statutory requirements for the use of video surveillance in foreign intelligence cases, the majority would leave video surveillance in all domestic law enforcement cases subject only to a few *ad hoc* constraints. In this respect, the majority seeks to solve the policy problem of its anomalous position by adopting in dicta some of the requirements of Title III as matters of constitutional law.³ There is no persuasive

³ The majority, however, imposes only four Title III requirements (at least insofar as dicta impose requirements), and these are not some of the most efficacious provisions. The majority does not require that only the Attorney General or a designated Assistant Attorney General authorize federal applications, § 2516(1), or that only the principal prosecuting attorney of a state (or of a political subdivision of a state if so authorized by

(Footnote continued on following page)

authority for this and, as a matter of judicial aggressiveness, it seems to me more egregious than a mere act of statutory interpretation. In any event, the constitutional requirements, which the majority imposes here by way of dicta can be, I suppose, just as easily interpreted away in the next case. I think it preferable to follow the mandates of 18 U.S.C. § 2511(2)(f) and 50 U.S.C. § 1809 and leave the matter to Congress.

Although there is no explicit mention of video surveillance techniques anywhere in Title III or in its legislative history, it is virtually inconceivable that the Congress which enacted Title III would have, if it had ever considered the question directly, left video surveillance unregulated by statute. The relevant committee reports and comments of individual members of Congress reflect quite clearly the process of balancing individual privacy concerns and the fight against organized crime. S. REP. NO. 1097, 90th Cong., 2d Sess. 67-69 (state of the law), 70-76 (balance between privacy and control of organized crime), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2154-56, 2157-63. The Johnson Administration and numerous members of Congress supported a total prohibition on wiretapping and electronic bugging, believing that the techniques would add relatively little in fighting crime and that the threat to privacy, especially if the techniques were abused, was too great to tolerate. S. REP. NO. 1097, 90th Cong., 2d Sess. 161-62, 172-73 (Johnson Administration supported *ban* on wiretaps and bugging), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2223-

continued

state law) may apply for a state order, § 2516(2). Thus, control over authorization is not centralized, and the power to apply for video surveillance orders is left in the hands of local law enforcement personnel. Nor does the majority impose the requirements of § 2516(1) & (2) which limit surveillance to the investigation of specified crimes. Further, the majority does not impose the strict statutory exclusionary rule of §§ 2515 and 2518(10)(a).

24, 2233-34. The proponents of Title III argued that the statute struck a correct balance between law enforcement and privacy interests. S. REP. NO. 1097, 90th Cong., 2d Sess. 186-87 (individual views of Sen. Bayh), 214-18 (individual views of Sen. Scott), 220 (individual views of Senator Eastland), 224-26 (minority statement), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2245-46, 2264-68, 2270, 2274-75. The only members of Congress who expressed opposition to Title III on the grounds that its provisions unduly restricted surveillance were several Senators who argued that the statute should not apply to state officials. S. REP. NO. 1097, 90th Cong., 2d Sess. 238-39 (individual views of Sens. Dirksen, Hruska and Thurmond), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2288-89.

Further, the committee reports reviewed the state of the law at the time and expressed deep dissatisfaction with the contemporary protection of individual privacy interests. S. REP. NO. 1097, 90th Cong., 2d Sess. 67-69, 162-64 (individual views of Sens. Long and Hart), 166-70 (additional views of Sen. Hart), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2154-56, 2224-26, 2227-31. The reports discussed at some length the Supreme Court's then-recent decisions in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967), and while they argued that Title III was constitutional, the reports also pointed out the inadequacies of then-applicable constitutional law decisions in protecting privacy. S. REP. NO. 1097, 90th Cong., 2d Sess. 66-76, *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2153-63. *But see id.* at 166-70 (additional views of Sen. Hart), *reprinted in* 1968 U.S. CODE CONG. & AD. NEWS 2112, 2227-31.

The clearest indications of this dissatisfaction are the statutory requirements which seem to go far beyond anything the Constitution demands. Those statutory

limitations and requirements include the following restrictions:

(1) bugging and wiretapping are permitted only when investigating specified crimes, 18 U.S.C. § 2516(1) & (2);

(2) authorization for bugging and wiretapping requests must be centralized in each jurisdiction so as to prevent local abuses and to make an identifiable person answerable for abuses, §§ 2516(1) & (2), 2518(1)(a);

(3) there is a statutory exclusionary rule for information obtained in violation of Title III, and that rule is broader than the constitutional exclusionary rule as it existed in 1968, let alone now, §§ 2515, 2518(10)(a);

(4) bugging and wiretapping must, in many instances, be disclosed to the targets after the investigation is concluded, § 2518(7) & (8)(d);

(5) police officers engaging in warrantless wiretapping or bugging are subject to criminal penalties, § 2511(1);

(6) targets of unlawful wiretapping and bugging have a private cause of action for damages, § 2520;

(7) the statutory requirements for minimizing obtrusiveness are much more specific than the Constitution requires, § 2518(1)(b) & (5); and

(8) bugging and wiretapping are permitted only when the government can show that conventional, less intrusive investigation techniques have proven or are very likely to prove unsuccessful, § 2518(1)(c) & (3)(e).

In 1968 Congress enacted Title III in part because audio surveillance was so intrusive that its use had to be

subjected to stringent statutory limitations. It is self-evident that the continuous video surveillance in the case before us is more intrusive by a wide margin. The combination of video and audio surveillance here let the government detect every sound, every word and every gesture—everything except the targets' unexpressed thoughts. Difficult as it may be to place ourselves in the position of Congress and accurately divine what it would have done in considering this new situation, we can say with some confidence what Congress would *not* have done. It would not have left video surveillance unregulated by statute if it had permitted it at all. In light of the political give and take on Title III, the flow of the debate, the way Congress arranged its agenda, the central competing policy concerns of proponents and opponents, we can say with confidence that Congress, if it had explicitly considered the prospect of video surveillance, would not have left it free of the constraints imposed on audio and wire surveillance. Yet the majority here does so, leaving the far more intrusive video techniques essentially subject only to a few *ad hoc* constitutional requirements which, by comparison, are ropes of sand.

The provisions and legislative history of the Foreign Intelligence Surveillance Act, enacted in 1978, lend additional support to this conclusion. FISA includes within its definition of "electronic surveillance" the use of video devices such as those used in the present case. 50 U.S.C. § 1801(f)(4); S. REP. NO. 604, 95th Cong., 1st Sess. 35, reprinted in 1978 U.S. CODE CONG. & AD. NEWS 3904, 3936; S. REP. NO. 701, 95th Cong., 2d Sess. 37, reprinted in 1978 U.S. CODE CONG. & AD. NEWS 3973, 4006.

FISA applies to investigations of special, and in some cases, extraordinary importance to the nation. See S. REP. NO. 604, 95th Cong., 1st Sess. 9, reprinted in 1978 U.S. CODE CONG. & AD. NEWS 3904, 3910. As was the case with Title III, the congressional debate was focused on achieving a correct balance, in this instance between privacy interests and national security. See S. REP. NO. 604, 95th Cong., 1st Sess. 7-9, reprinted in 1978 U.S. CODE CONG. &

AD. NEWS 3904, 3908-10; S. REP. NO. 701, 95th Cong., 2d Sess. 16, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3973, 3985. In 1978 Congress was willing to authorize the use of these extremely intrusive video surveillance devices, but only subject to conditions which are, in some ways, even more strict than those contained in Title III. For example, only the Attorney General or Deputy Attorney General may apply for a court order under 50 U.S.C. § 1804(a). The need for the surveillance and its relation to foreign intelligence must be certified by the President's adviser for national security affairs or by a national security official whose appointment is subject to Senate confirmation. § 1804(a)(7)⁴. The statute draws on Title III as its model on issues of necessity and minimization, and imposes those more stringent non-constitutional requirements. § 1805(b) & (d). The surveillance must be carried out subject to court order and supervision, S. REP. NO. 604, 95th Cong., 1st Sess. 16, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3917-18, and the court is a special one selected by the Chief Justice of the United States, § 1803(a), to develop expertise in the subject matter and to impose some controls on the executive branch in conducting this type of surveillance. S. REP. NO. 604, 95th Cong., 1st Sess. 16, *reprinted in* 1978 U.S. CODE CONG. & AD. NEWS 3904, 3917. The court operates in secret but it is still an Article III court with the authority to deny permission for surveillance.

Congress was so concerned about potential abuses of these investigative techniques in foreign intelligence cases that it imposed these numerous requirements — checks and balances affecting officials at the highest levels of government. It imposed those requirements in cases of utmost importance and sensitivity to national security. I am unpersuaded by the suggestion that Congress could

⁴ There are special limited provisions for warrantless surveillance under very narrow circumstances on orders of the President and certification by the Attorney General. 50 U.S.C. § 1802 (a).

have subjected these techniques to such tight controls in those cases and still left open the use of the same techniques for every local police department in every minor investigation. The majority's interpretation would presumably give the power to engage in this intrusive video surveillance to virtually any officer with a badge and to any official with a robe and gavel. In fact, the majority runs the risk of leaving open the use of video surveillance with such relatively loose controls in every case *except* those of greatest importance. According to the majority, Congress entrusted powers to a deputy sheriff and half-time magistrate on a local gambling investigation that it expressly denied the director of the Federal Bureau of Investigation and a special expert court in foreign intelligence cases of the utmost sensitivity and importance. This result is irrational and contrary to Congressional intent. If statutory language must be bent, as the majority must bend the language of 18 U.S.C. § 2511(2)(f) and 50 U.S.C. § 1809, we should at least bend it in the general direction of Congressional purpose and method.

The defendants make a plausible argument, based on the statutory language, for a third interpretation of FISA and Title III, under which video surveillance is prohibited except in foreign intelligence cases.⁵ I cannot dismiss defendants' argument out of hand; indeed I have argued consistently with it that FISA and Title III are constructed to provide a comprehensive framework for the use of electronic surveillance in the United States in situations

⁵ A similar argument, that the absence of provisions in Title III for video surveillance implies that such surveillance is forbidden, has been rejected as giving too little weight to Congressional concerns. *In re Application for Order Authorizing Interceptions of Oral Communications and Videotape Surveillance*, 513 F. Supp. 421, 422 (D. Mass. 1980) (allowing video surveillance where substantive safeguards at least as rigorous as those required by Title III, if not more so, had been observed). The effect of FISA on Title III was not considered.

where the targets have a reasonable expectation of privacy. Under that scheme the government's use of video surveillance in this case was illegal if it was not authorized either by FISA or by Title III.

It is obvious that the government's video surveillance here was not authorized under FISA. The FALN is not a "foreign" target within the meaning of FISA and the government made no attempt to employ FISA procedures. Therefore, either Title III must apply or the video surveillance was unlawful.

But the defendants argue that Title III cannot authorize video surveillance because that statute is limited to audio and wire surveillance, as appears in the language of 18 U.S.C. §§ 2510 and 2511.⁴ This language, in particular the definition of "intercept" contained in 18 U.S.C. § 2510(4), does indeed pose the principal obstacle to reaching my conclusion. That definition states: "'intercept' means the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device." On its face, this definition appears to restrict Title III to audio surveillance techniques, and courts have construed the definition as limited to devices which acquire information through the sense of hearing. *E.g., United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977) (pen registers); *United States v. Cassidy*, 546 F. Supp. 611, 621 (E.D. Mich. 1981) (beepers), *rev'd in part, on other grounds*, 720 F.2d 451 (6th Cir. 1983), *vacated* 104 S. Ct. 3581 (1984) (mem.). Three courts have specifically held Title III not applicable to video surveillance. *In re Application for Order Authorizing Interception of Oral Communications and Videotape Surveillance*, 513 F. Supp. 421 (D.Mass. 1980); *People v. Teicher*, 52 N.Y.2d 638, 422 N.E.2d 506 (1981); *Sponick v. City of Detroit Police Dept.*, 49 Mich. App. 162, 211 N.W.2d 674 (1973).

Both the majority and the government agree, though they draw a different conclusion than do the defendants.

There are, however, several reasons why we should not adhere blindly to those prior constructions. First, the prior court constructions have, with certain exceptions, involved efforts by defendants to extend Title III to relatively *less* intrusive surveillance devices such as pen registers, which record telephone numbers dialed by a monitored telephone. See *New York Telephone, supra*, and cases cited therein at 166 n.9; *Cassity, supra*. Courts have with good reason relied on both the language of the statute and the legislative history to resist extensions of Title III to these less intrusive surveillance methods. The definition of "intercept" in Title III is carefully worded, but its sharp focus on the "aural" acquisition of information was designed to avoid including *less* intrusive surveillance devices. S. REP. NO. 1097, 90th Cong., 2d Sess. 90, reprinted in 1968 U.S. CODE CONG. & AD. NEWS 2112, 2178. The use of the word "aural" had the effect of limiting Title III to those highly intrusive electronic surveillance measures, such as wiretapping and bugging, which could disclose the *contents* of communications. *Id.*

The question we face here, by contrast, is one which the definition of "intercept" was not framed to address. We are dealing with a far more intrusive surveillance technique, and one that surely has the effect of revealing the contents of communications together with a vast amount of other information about targets. Careful wording does not require us to reach irrational results when facing a question not contemplated by the drafters of the definition merely because other courts have reached those results in a different context.

In addition, whatever the scope of Title III before 1978, the enactment of FISA in 1978 provides a sound basis for extending Title III to encompass video surveillance.⁷ Because FISA was intended to mesh with Title III

⁷ None of the courts which have said Title III is limited to information acquired through the sense of hearing has consid-

(Footnote continued on following page)

in a comprehensive statutory system for regulating highly intrusive forms of electronic surveillance, it included a number of "conforming amendments" to prevent various statutory anomalies or conflicts which might otherwise have arisen.⁷ Some of those conforming amendments expressly introduced the FISA definition of "electronic surveillance" (including its video dimension) into some sections of Title III. *E.g.*, FISA § 201(a), amending 18 U.S.C. § 2511(2)(a)(ii) (authorizing a common carrier to assist an agent with a court order authorizing the interception of wire or oral communications or electronic surveillance as defined in FISA).

The inclusion of video surveillance in FISA's definition of electronic surveillance is relatively obscure and

continued

ered the complicated effects of the 1978 FISA statute, which quite clearly does cover video surveillance. *E.g.* *United States v. New York Tel. Co.*, 434 U.S. 159, 165-68 (1977) (pen registers); *United States v. Cassity*, 546 F. Supp. 611, 621 (E.D. Mich. 1981) (beepers), *rev'd in part, on other grounds*, 720 F.2d 451 (6th Cir. 1983), *vacated* 104 S. Ct. 3581 (1984)(mem.). Nor have the effects of FISA on Title III been considered by the three courts which have held Title III inapplicable to video surveillance. *In re Application for Order Authorizing Interception of Oral Communications and Videotape Surveillance*, 513 F. Supp. 421 (D. Mass. 1980); *People v. Teicher*, 52 N.Y.2d 638, 422 N.E.2d 506 (1981); *Sponick v. City of Detroit Police Dept.*, 49 Mich. App. 162, 211 N.W.2d 674 (1973). Several of the cases relied on by the majority, including *New York Telephone* and *Sponick*, were decided prior to the enactment of FISA. And in *In re Application*, Judge Keeton allowed video surveillance only after forcing the government to go through Title III application procedures and subjecting the surveillance to substantive safeguards at least as rigorous as those required by Title III. *In re Application*, 513 F. Supp. at 423.

⁷ These undesirable effects included such possible results as holding federal agents criminally liable under 18 U.S.C. § 2511 for acting in accordance with a court order under FISA. See FISA § 201(b).

becomes explicit only in a few sentences buried in the committee reports. Congress' attention was clearly elsewhere with regard to FISA. And it seems evident to me that the potential problems of either the majority position or the defendants' position were simply not recognized in the development of one complicated statute and its integration with another complicated statute. Either result—the exemption of video surveillance from any statutory regulation or the prohibition of video surveillance—is extreme enough to persuade me that Congress, if it had noticed the possibility, would at least have commented on it somewhere. Instead, there is silence.

In view of the language of both Title III and FISA, the purposes of both statutes, the practical connections between audio and video surveillance methods and the silence in the legislative history on the subject, it is most sensible to view the statutory dilemma as the result of inadvertence rather than design. FISA's "conforming amendments" simply did not mesh the gears of the statutes quite as smoothly as Congress had intended.

There is a further difficulty with the defendants' argument. If Congress chose to prohibit video surveillance, it chose a remarkably roundabout and subtle way to do it, and it never indicated clearly any intention to do so. In fact, neither Title III nor FISA *prohibits any* specific surveillance method. Instead, both statutes are designed to *control* intrusive methods of electronic surveillance by regulating their use. There is no indication in the language or legislative history of either statute that Congress meant to outlaw *any* form of surveillance, and I think it quite implausible that Congress—faced with a situation such as confronts us—would have prohibited surveillance in almost any form.

Although the defendants' argument is certainly not frivolous, and, indeed, tracks the statutory language more closely than the interpretations offered in this and the

majority opinions, we should, in order to avoid absurd results, construe Title III to apply to video surveillance for domestic law enforcement investigations where the targets of the surveillance have a reasonable expectation of privacy, as in this case.

As a practical matter, the procedural and substantive requirements of Title III are compatible with video surveillance in every respect, and video surveillance is likely to be used only in tandem with audio surveillance techniques already subject to Title III. The same application, the same authorization, the same showing of probable cause, the same showing of need for such intrusive measures would all apply equally to both video and audio surveillance methods. And, of course, that is essentially the course the government pursued here in its applications, including a request for video surveillance as part—albeit as only one sentence—of routine Title III applications.⁹ Thus, the details of the Title III regulatory scheme appear to be compatible in every respect with video surveillance as a supplement to audio surveillance.

Further, the application of Title III to video surveillance seems to me to be most closely in accord with Congress' intent in Title III and FISA. Congress was troubled by the potential for abuses of electronic surveillance, and was dissatisfied with the adequacy of the contemporary constitutional doctrine for the protection of privacy interests. The purpose of these two statutes was not to outlaw electronic surveillance but to subject it to rigorous controls. A key element of both Title III and FISA is that each centralizes authority *and responsibility* for the use of intrusive means of electronic surveillance. Congress was quite concerned in Title III to prevent the possibility of local or relatively low-level officials using or abusing their power by employing electronic surveillance for their own purposes, or where it was otherwise unwar-

⁹ This course was also taken by the government, though after some prodding by Judge Keeton, in *In re Application*, *supra*.

ranted. There is of course no guarantee that high level officials will not also abuse their power, but Title III was designed to make it easy to assign responsibility for abuses and to provide for rational and consistent policies in the use of these highly intrusive measures. All of these concerns apply with *at least* as much force to video as to audio surveillance and it makes the utmost sense to apply those constraints to video surveillance as well.

Of course, this is open to criticism as an aggressive exercise in statutory construction, and if either of the alternatives were more consistent with *both* statutes and their purposes and legislative histories, I would perhaps retreat from my interpretation. However, each alternative has technical and policy problems which are, in my view, considerably more severe than my bending of the Title III language. If my construction were to be chastised as "result oriented," I would assert that it seeks a result which is both sensible and consistent with both the statutes and the legislative histories read carefully and as a whole. Applying Title III to video surveillance avoids the majority's anomaly of subjecting the most dangerously intrusive form of electronic surveillance to much less control¹⁰ than other forms. In addition, the majority's interpretation subjects video surveillance to much less control in the investigation of a local gambling parlor than in foreign intelligence investigations. My construction also avoids the improbable result of reading Title III and FISA as prohibiting one particular form of electronic surveillance when there are no indications anywhere that Congress meant to prohibit any surveillance technique in all situations. Instead, my approach subjects this highly intrusive form of surveillance to at least as much constraint as less intrusive forms are subject to, and it accords with the general congressional design of closely regulating—not prohibiting—these somewhat awesome forms of surveillance.

¹⁰ See n.3 *supra*.

UNITED STATES v. BOWLER

1323

Cite as 561 F.2d 1323 (1977)

We do not imply that there is an *ipso facto* exemption for those who transport undocumented aliens for employment or as an incident to employment. See *United States v. Acosta de Evans*, 531 F.2d 428 (9th Cir. 1976).

[4] We merely state that where the transportation of such an alien occurs, there must be a direct or substantial relationship between that transportation and its furtherance of the alien's presence in the United States. Even though the qualification in the transportation section ("in furtherance of such violation of law") does not provide the automatic exclusion in the employment situation which the proviso in the harboring section does, it still requires, if it is to have any meaning at all, that a direct or substantial relationship exist.

[5] While the parameters of § 1324(a)(2) are not precise, we must be guided by the nature of the statute as well as the legislative intent for its enactment. As a penal statute, it must be strictly construed. *McBoyle v. United States*, 283 U.S. 25, 51 S.Ct. 340, 75 L.Ed. 816 (1930); *United States v. Fruit Growers Co.*, 279 U.S. 363, 49 S.Ct. 374, 73 L.Ed. 739 (1928).

This court in *Gonzalez-Hernandez*, *supra*, left open exactly what constitutes in furtherance of the alien's violation of the law under § 1324(a)(2). 534 F.2d at 1354. There, defendant's relationship to the actual illegal entrance seemed much more direct and substantial as to time, place, distance and overall impact than does the case before us. Thus, the result in *Gonzalez-Hernandez* is consistent with the test set forth by this court herein.

A broader interpretation of the transportation section would render the qualification placed there by Congress a nullity. To do this would potentially have tragic consequences for many American citizens who come into daily contact with undocumented aliens and who, with no evil or criminal intent, intermingle with them socially or otherwise. It could only exacerbate the plight of these aliens and, without adding anything significant to solving the problem, create, in effect judicially, a new crime and a new class of criminals. All of our free-

dom and dignity as people would be so reduced.

Reversed.



UNITED STATES of America,
Plaintiff-Appellee,

v.

Patrick Earl BOWLER,
Defendant-Appellant.

No. 76-2713.

United States Court of Appeals,
Ninth Circuit.

Sept. 30, 1977.

Defendant was convicted before the United States District Court for the District of Arizona, C. A. Muecke, J., of fraud by wire, and he appealed. The Court of Appeals, East, Senior District Judge, sitting by designation, held that: (1) telephone company's use of a snifter in investigation of illegal use of blue box did not violate Title III of the Omnibus Crime Control and Safe Streets Act of 1968, since a snifter only records each telephone emission of a 2,600 cycle tone, and is incapable of making an aural acquisition of communications; (2) where search warrant and supporting affidavit described physical appearance of defendant's residence and listed street address as 3835 West Diana Avenue, but true street address was 3335 West Diana Avenue, and correct street address was specified in statement of probable cause attached to and incorporated into affidavit, magistrate properly corrected typographical error in search warrant and affidavit when FBI agent brought such error to magistrate's attention, and (3) evidence sustained finding that defendant not only understood his *Miranda* rights but exercised them intelligently, freely and voluntarily, and that statements made by defendant after administration of *Miranda* warnings were not

tainted by statements improperly adduced before such warnings were given.

Affirmed.

1. Telecommunications ⇐494

Telephone company's use of a snifter in investigation of illegal use of blue box did not violate Title III of the Omnibus Crime Control and Safe Streets Act of 1968, since a snifter only records each telephone emission of a 2,600 cycle tone, and is incapable of making an aural acquisition of communications. 18 U.S.C.A. §§ 2510 et seq., 2511(1)(c), (2)(a)(i), 2515.

2. Searches and Seizures ⇐3.5

Where search warrant and supporting affidavit described physical appearance of defendant's residence and listed street address as 3835 West Diana Avenue, but true street address was 3335 West Diana Avenue, and correct street address was specified in statement of probable cause attached to and incorporated into affidavit, magistrate properly corrected typographical error in search warrant and affidavit when FBI agent brought such error to magistrate's attention. Fed.Rules Crim.Proc. rule 41(c), 18 U.S.C.A.; U.S.C.A.Const. Amend. 4.

3. Searches and Seizures ⇐3.5, 7(6)

Neither Fourth Amendment nor Federal Rules of Criminal Procedure nor case law requires a person to be sworn or resworn before bringing a typographical error to attention of issuing magistrate prior to the execution of search warrant, where correct information is already properly before magistrate. Fed.Rules Crim.Proc. rule 41(c), 18 U.S.C.A.; U.S.C.A.Const. Amend. 4.

* Honorable William G. East, Senior United States District Judge for the District of Oregon, sitting by designation.

1. The Bell Telephone System uses the 2,600 hertz cycle tone to control its long distance network. No such tone should be emitted from a private telephone at any time. A blue box emits a 2,600 cycle tone and is used to circumvent the toll call billing system of the phone company.

4. Criminal Law ⇐414

Evidence in prosecution for fraud by wire sustained finding that defendant not only understood his *Miranda* rights, but exercised them intelligently, freely and voluntarily, and that statements made after administration of *Miranda* warnings were not tainted by statements improperly adduced before warnings were given.

Michael E. Benchoff, Phoenix, Ariz., argued for defendant-appellant.

Daniel R. Drake, Asst. U. S. Atty., Phoenix, Ariz., argued for plaintiff-appellee.

Appeal from the United States District Court for the District of Arizona.

Before BARNES and KILKENNY, Senior Circuit Judges, and EAST,* Senior District Judge.

EAST, Senior District Judge:

Patrick Bowler (Bowler) was indicted under six alleged counts of violating 18 U.S.C. § 1343, fraud by wire. The essence of the charges was that Bowler had used a "blue box"¹ to defraud the Mountain Bell Telephone Company (Bell) of money due for interstate telephone calls placed by Bowler.

After a hearing on Bowler's motion to suppress the use of certain evidence, the case was tried to the District Court without a jury which found him guilty on all counts.² Bowler was placed on four years probation as to each count with the requirement that he make restitution to Bell of \$900.00.

On appeal, Bowler raises three issues regarding the admissibility of evidence. We affirm.

Bowler first came to the attention of Bell during an investigation of Donald Anderson, a fellow employee of Bowler's, for blue box toll fraud. An "Hekemian"³ attached

2. The District Court ordered that admissions made by Bowler prior to the administration of the *Miranda* warnings be suppressed; in all other respects the motion was denied.

3. An Hekemian is a device which records the number dialed, the date and the time a call originates and terminates. Upon detection of a 2,600 cycle tone, it also prints the information in red and starts a tape recorder which runs for less than two minutes. Thus, the Hekemian is designed to generate "paper tapes" which pro-

UNITED STATES v. BOWLER

1325

Cite as 561 F.2d 1323 (1977)

to Anderson's telephone showed that he had made several telephone calls to Bowler's number. David Burkhart, a security officer for Bell, placed a "snifter"⁴ on Bowler's telephone solely because the Anderson tapes revealed the calls to Bowler's home. Bell maintained a common practice of checking out "known associates" of blue box users. The snifter revealed that 2,600 cycle tones were being emitted by Bowler's telephone and accordingly an Hekemian was attached thereto. The evidence gathered by it indicated illegal toll calls were being placed by Bowler. Burkhart then turned his information over to the Federal Bureau of Investigation.

Based on the information supplied by Burkhart, Agent Gwin of the F.B.I. obtained a warrant to search Bowler's home. Execution of the warrant led to the discovery of a blue box and statements were taken from Bowler before and after he received *Miranda* warnings.

[1] Bowler first complains that no evidence was properly admitted against him because it was all derived from the use of the snifter which on the facts of this case constituted random monitoring in violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, § 802, 18 U.S.C. § 2511(2)(a)(i) (1970).⁵ However, this argument has no merit since the use of a snifter is not within the scope of Title III.

The snifter does no more than record each telephone emission of a 2,600 cycle tone characteristic of the illegal use of a blue box. The use of such a device is not

vide a basis for restitution by supplying evidence that a toll call was made and indicating the parties involved.

4. The sole function of a snifter is to "peg a register" each time it detects a 2,600 cycle tone. It records neither the number called nor the content of any communications made.

5. Fourth Amendment standards are not involved in assessing the propriety of this action because Burkhart did not act in concert, under the direction or with the acquiescence of state or federal officials.

restricted by § 2511(2)(a)(i) because "the right of privacy protected by the wire tap statutes goes to message content rather than the fact that a call was placed." *United States v. Goldstein*, 532 F.2d 1305, 1312 (9th Cir. 1976). This conclusion is further buttressed by a more recent decision of this Court. In *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F.2d 254 (9th Cir. 1977), this Court noted that Title III only prohibits disclosure and use of communications which are "intercepted" within the meaning of the Act and that the term "intercept" covers only "aural acquisitions" of communications. *Id.* at 257. The Court then held "that the use of [a] pen register [does] not constitute a violation of Title III . . . [b]ecause a pen register is incapable of making an aural acquisition of any communication . . ." *Id.*

"A pen register records the numbers dialed from a particular telephone. It does not disclose the contents of any conversation nor does it indicate whether any calls were completed." *Id.* at 266, Hufstedler, J. concurring. In contrast, the snifter does not even record the number dialed and the appellant justly concedes that a snifter is "less intrusive than even a pen-register . . ." Since the use of the more intrusive pen register is not governed by Title III, it follows that the use of the snifter is also outside the ambit of the Act.⁶

Bowler's second argument is that the search warrant was defective in that an attempt to correct an error in the description of the premises to be searched was "legally insufficient" and that the uncor-

If, however, Bell violated the Act in obtaining the contents of any of Bowler's communications, 18 U.S.C. § 2511(1)(c) would make disclosure thereof unlawful and the introduction into evidence of the contents or any evidence derived therefrom would be prohibited by 18 U.S.C. § 2515.

6. Once Bell had the information supplied by the snifter, its action in attaching the Hekemian—which device is capable of making aural acquisitions of communications—clearly was not unlawful random monitoring as provided in 18 U.S.C. § 2511(2)(a)(i). *Goldstein*, 532 F.2d at 1313.

rected description failed to satisfy the particularity requirement of the Fourth Amendment. The search warrant and supporting affidavit described the physical appearance of Bowler's residence and listed the street address as 3835 West Diana Avenue, Phoenix, Arizona. However, the true street address was 3335 West Diana Avenue. Prior to the execution of the warrant, Agent Gwin noticed the error and brought it to the attention of the issuing magistrate who promptly corrected the affidavit and the warrant.

Bowler claims that the actions of Agent Gwin constituted "oral testimony" not sworn and made a part of the affidavit as required by Fed.R.Crim.P. 41(c) and *United States v. Anderson*, 453 F.2d 174 (9th Cir. 1971). The flaw in Bowler's argument is that the accurate information was properly before the magistrate at the time the correction was made. The correct street address was specified in a "Statement of Probable Cause" which was physically attached to and incorporated into the affidavit. Thus, the correct address had been properly sworn to before the magistrate. *United States v. Buschman*, 386 F.Supp. 822, 829 (E.D.Wis.1975), *aff'd*, 527 F.2d 1082 (7th Cir. 1976).

[2, 3] The District Court found the magistrate had merely corrected a "clerical error." It appears and we agree that the District Court rightly concluded that the correct address was specified in the "Statement of Probable Cause" and that a typographical error in the first part of the affidavit was carried over to the search warrant. Corrections of such errors are perfectly proper. *United States v. Keach*, 480 F.2d 1274, 1284-85 (10th Cir. 1973); *United States v. Pittman*, 439 F.2d 906, 909 (5th Cir.), *cert. denied*, 404 U.S. 842, 92 S.Ct. 138, 30 L.Ed.2d 77 (1971). Neither the Fourth Amendment nor Rule 41(c) nor *Anderson*

7. Since we hold that the description of the premises to be searched was properly corrected, we need not discuss Bowler's further con-

nor common sense requires a person to be sworn or resworn before bringing a typographical error to the attention of the issuing magistrate prior to the execution of the warrant where the correct information is already properly before him.⁷

[4] Bowler's final contention is that the statements he made after the administration of the *Miranda* warnings were not properly admitted because they were tainted by statements improperly adduced before the warnings were given. The District Court found that Bowler not only understood his rights but exercised them intelligently, freely and voluntarily, answering some questions while refusing to answer others. This finding, which was based upon evidence brought out at the hearing on the motion to suppress, involved a determination of the credibility of conflicting testimony and consideration of Bowler's age, education, mental condition and articulateness, as well as the particular setting in which the statements were given. We are not convinced that "the conditions that rendered the pre-warning admissions inadmissible carried over to invalidate [his] subsequent confession." *United States v. Toral*, 536 F.2d 893, 896 (9th Cir. 1976).

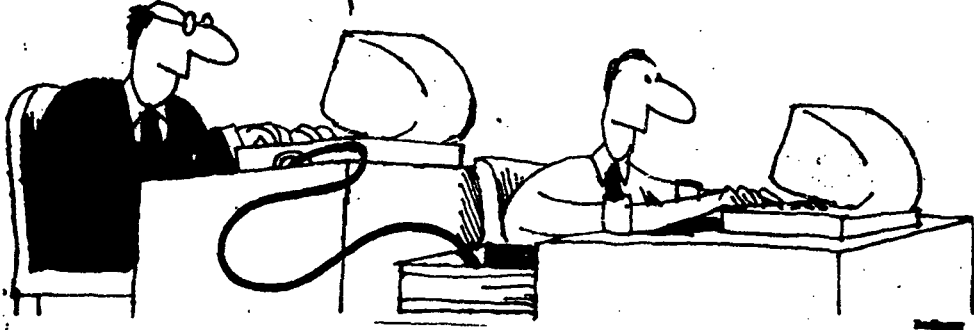
The judgment of conviction and suspended sentence of Bowler entered by the District Court on July 19, 1976 is affirmed.

AFFIRMED.



tion that the description, uncorrected, was inadequate.

Can Privacy and Computer Coexist?



By DAVID BURNHAM

Special to The New York Times

WASHINGTON, Nov. 4—Should a Federal agency have the right to search an employee's personal material filed in a Government computer?

Is such a search comparable to searching desk drawers to see if they contain personal notes or papers?

These were some of the questions that Larry Layton, a 38-year-old civilian computer official with eight years' experience at the Army's Materiel Development and Readiness Command, decided needed examination.

So, a few weeks ago, Mr. Layton sat at his computer terminal and tapped out a message for the national electronic mail system established by the Defense Department to help scientists all over the country communicate with each other about nonclassified matters of common interest.

Complaint About Investigation

He informed all those with access to what is called the ARPA Net, for Advanced Research Projects Agency, that his interest in these questions about such searches had been touched off by three instances where the Army's Criminal Investigation Division, sometimes in conjunction with the Federal Bureau of Investigation, had made total inspections "of our workplace computers without any type of court order or identification of what they are looking for other than 'wrongful use of Government property.'"

The investigators, he added, had not limited their search to specific individuals or files.

The computer expert continued, saying that he knew of employees who had been bedeviled by the investigators for seemingly insignificant violations of Government policy.

"They have read individuals their

rights and otherwise tried to intimidate them in two instances that I know of, once after finding a recipe in a message, and once, when a baby sitter's telephone number was found in a telephone number file," he said.

"I just thought some problems were raised that should be considered by the Government, academic and industry people who have access to ARPA Net," he explained Wednesday in an interview.

Tip About Missing Computer

An spokesman for the Army's Criminal Investigation Division, Marilyn Love, refused to answer a list of specific questions raised by Mr. Layton's statement. She said it was against Army policy to comment on "on-going investigations." She added that the cases referred to by Mr. Layton were discovered as a result of a tip received by investigators in December 1982 that Army employees were misusing the computer.

Mr. Layton said in his message that the Army's legal staff had advised his supervisors "that what is taking place is legal, by all precedents." He added, "They say that computer files do not have the same privacy protection that telephone usage has."

The message continued, "If in fact, the owner of a computer system has the right to search (in a witch hunt fashion) through all the files, with the threat of prosecution, then I too will refrain from using the system as I have in the past: as a note pad, telephone replacement, sounding board for ideas, etc."

Emphasizing that he was speaking for himself, and not the Army, he ended his message with this plea for information: "Does anyone out there know where the law is heading in this type of issue? I would hope that '1984' is not as close as it appears."

The responses he got were not very comforting. Mark Crimbs, who identified himself as being associated

with Stanford University in California, replied via the ARPA net that his experiences suggested that these freedoms or privacy that manage to exist do so solely because of "the good will of those in power," adding, "Regrettably, many computer centers are run by various flavors of petty dictators."

Several days later, Stephen Wall, who did not mention the institution he worked for, chipped in that in the Government agency where he worked he was not permitted to make baby sitter arrangements during working hours. "I can loose my job for using the taxpayers' telephone for my personal business," he said. "It's no hardship though, there's a perfectly good pay phone in another building not 200 yards from my office."

Matters of Ethics and Fraud

Geoffrey S. Goodfellow, who also did not indicate where he worked, was more sympathetic. He sent through the ARPA net a parody of a *Street News* article in which a Government department with the acronym of "Dumbb" undertook an investigation of "unauthorized desk contents," which resulted in the dismissal of several employees when aspirin, candy, personal letters and a bowling team roster were found in their desks.

Despite the difficult ethical questions raised by the new computer systems, however, the Government has pushed ahead with its investigations of computer-related fraud and abuse.

In testimony before the Senate Government Affairs Oversight Subcommittee, Richard P. Shusterman, chief inspector general of the Department of Health and Human Services, announced a recent survey discovered misuses in 12 different Federal agencies where Government computers were used for entirely business-unrelated purposes. One employee, for example, ran his football pool on his company's computer, while another operated a thriving consulting business.

Computer Communications Vulnerable As Privacy Laws Lag Behind Technology

No federal law clearly makes it a crime to intercept computer transmissions or to break into a computer system to look around or destroy information.

BY RONALD BROWNSTEIN

When Citicorp vice president Richard W. Coughenour wants to send a memorandum to one of the bank's employees, he turns to a compact device on the corner of his desk that looks like a cross between a computer and a telephone. The machine, called a Displayphone, has the typewriter-like keyboard and video display screen of a computer and the touch sensitive key pad of a fancy telephone.

Coughenour hits a touch pad labeled EZmail and the machine dials the number to connect him with Citicorp's internal electronic mail system, the electronic tones softly tolling as the Displayphone runs through the digits. When the number is dialed, Coughenour hits a touch pad labeled connect and the screen lights up with commands. First it asks him to enter his mailbox number. Then it asks for his password.

To send a memo, Coughenour hits a touch pad labeled compose and pulls out the small keyboard from under the pad. He types out the message and hits the touch pad labeled send.

From his office at the tip of Wall Street, the message skitters across the bank's private fiber optic cables to Citicorp's Park Ave. office. From there, if it is traveling to a Citicorp office outside New York City, the message rides a microwave relay to a private earth station in New Jersey where it is transmitted 22,300 miles up to a satellite on which Citicorp owns space. From the satellite, the message returns to another Citicorp earth station and then along public or leased phone lines to the recipient's computer. All in a matter of seconds.

Although the message is easy to send, it is also easy to steal. With a large enough antenna, it is not difficult to intercept microwave transmissions.

Is anybody listening in? "I don't doubt it," said Coughenour, a former Air Force intelligence officer who runs Citicorp's mail services. "The Russians have a big mission at the United Nations and all that equipment on the roof; that's not all there to get Home Box Office. I don't wonder if [some of our competitors] are pointing some stuff at us too."

The information may be vulnerable in a legal sense as well. While the laws governing wiretapping clearly protect spoken communications—essentially, ordinary telephone calls—many experts are concerned that no law makes it a crime to eavesdrop on communications between two computers, even though the information that passes between them is often highly sensitive.

The fuzziness of the laws protecting computer-to-computer communications is only one area where new computer or communications technologies, or merely new and aggressive applications of existing technologies, have exposed gray spots in the nation's laws governing privacy. "Our laws have not kept pace with the technology," said attorney Ronald L. Plesser, former general counsel of the Privacy Protection Study Commission, which studied the nation's privacy laws for Congress in the mid-1970s. "The technology has been expanding so quickly that the laws written for one level of technology quickly become obsolete."

Generally, the privacy implications of these technological changes have not received much political, legal or social attention. "We're not even giving it serious, practical consideration," said University of Illinois political economy professor David F. Linowes, who chaired the privacy commission.

But with the arrival of George Orwell's nightmare year of 1984, these blind spots in the law and the general issue of privacy are beginning to receive increased scrutiny.

New York Times reporter David Burnham has reignited a debate on the potential threat to privacy posed by the use of computers with a controversial new book, *The Rise of the Computer State*. Robert W. Kastenmeier, D-Wis., who chairs the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, has begun a wide-ranging series of hearings on the state of civil liberties, including the impact of new technology on privacy. Several other committees are examining the laws safeguarding computer information. Universities and other organizations across the country, such as the Smithsonian Institution, are holding conferences on Orwell, technology and 1984. And the American Civil Liberties Union is planning a major conference on privacy.

Many of these forums will be used to criticize the Reagan Administration's policies on release of government information, classification of government documents and law enforcement. But most of these groups are also examining a different issue: where has new technology outflanked the privacy laws?

ELECTRONIC MAIL

A new technology almost entirely unaddressed by existing law is electronic mail. For years, communications experts have considered electronic mail—generally defined as the electronic transfer of written information—to be a tool of tremendous potential. Electronic mail allows an executive such as Coughenour to send messages instantly to employees around the world, far faster than by any courier service.

But the potential of electronic mail has largely been unrealized. Private electronic mail services did only about \$40 million worth of business in 1983, and the few companies with their own internal systems, of which Citicorp is considered a

leader, sent about an equivalent number of messages, estimates Kenneth G. Bosomworth, president of International Resource Development Inc., an electronic mail consulting firm. Growth has been slow because the electronic mail systems have generally required both the sender and recipient of a communication not only to have computers but also to subscribe to the same system.

Industry observers expect that electronic mail will take off with MCI Communications Corp.'s entry into the business. In September, MCI launched an electronic mail service that allows anyone with a computer terminal, or even an electronic typewriter, to send a message to anyone else in the United States. If the recipient does not have a terminal, the message is printed nearby and delivered either by courier or the U.S. Postal Service.

MCI is predicting rapid growth for the system: from 80,000 users today to 200,000 by 1985. And industry experts are inclined to agree. "The MCI entry will transform the industry's revenue picture," said Bosomworth.

With the proliferation of computer terminals in the home and the office, electronic mail could eventually siphon off a significant chunk of both mail and telephone business. In 1982, the congressional Office of Technology Assessment calculated that ultimately at least two-thirds of the Postal Service's annual volume of 110 billion pieces "could be handled electronically." By 1990, the office estimated, more than 23 billion messages could be sent through electronic mail or electronic funds transfer systems. The report predicted that conventional mail volume is likely to peak in the next decade and then decline.

Though the economic prospects for electronic mail may be starting to clear up, the laws covering it remain cloudy in two basic areas: unauthorized entry into such systems and requests by law enforcement officials for access to the records of people's communications held by electronic mail networks, such as MCI. The legal uncertainty underscores the major privacy concern of electronic mail's potential customers, who are worried about competitors reading their internal communications. "The fear [among possible users] is that somebody will get access to the system's central computer and get access to their messages," said computer consultant Walter E. Ulrich, who chairs the new Electronic Mail Association's committee on privacy.

Prosecutors have complained that while existing laws can be used against criminals who use computers to commit fraud, no law clearly makes it a crime to break into a computer system to look



In a matter of seconds, Citicorp vice president Richard W. Coughenour sends messages on his Displayphone from his office on Wall Street to bank employees around the world. Although the message is easy to send, it is also easy to steal.

around or destroy information. Some legal barriers are in place. About 20 states have laws addressing unauthorized computer break-ins, and some experts note that if someone sought unauthorized entry into a computer system by misrepresenting himself as an authorized user he could be prosecuted under the federal wire fraud law.

But the electronic mail industry, among other computer users, would like clearer protection. The wire fraud law "was not designed for the problem of trespassing against someone's intellectual or electronic property," said Jack Greenberg, general counsel of GTE Telenet Communications Corp. Telenet runs a private electronic mail system used by 130 companies that was broken into repeatedly last summer, most notably by a group of Milwaukee teenagers using home computers.

Rep. Bill Nelson, D-Fla., and Sen. Paul S. Trible Jr., R-Va., have introduced identical bills (HR 1092, S 1733) that would make it a federal crime to "take something of value" from a computer or to damage the information in it. Nelson's bill has also been incorporated into legislation pending before the Judiciary Subcommittee on Crime that addresses credit card fraud. Both the Nelson and Trible bills, though, still would not make it a crime to enter a computer system and look at the data in it. An aide to Nelson said the bill's sponsors did not believe that should be a federal crime.

While Congress slowly considers these proposed legal barriers to computer break-ins, electronic mail companies have been beefing up their technical defenses. In October, the Defense Department split the 15-year-old ARPAnet, an

electronic mail network run by the Advanced Research Projects Agency, into separate systems for military and unclassified civilian research to further limit access to military secrets. Unlike other systems, the new MCI mail will not allow users to pick their own passwords—which are often no more sophisticated than the name of the user's spouse. Instead the new system assigns passwords that are randomly generated.

The electronic mail operators have also installed systems to prevent would-be intruders from programming their own computers to repeatedly try possible passwords until one clicks. Usually, the systems disconnect a user after three unsuccessful attempts at the proper password. After three such disconnections, the MCI system is programmed to notify the firm's security department.

Citicorp's system has similar security protections. But no system is immune to penetration, said Coughenour, who noted that break-in attempts occur "all the time." The ultimate defense, he said, can only be to keep sensitive information out of the electronic mail system. "Users of the system understand it and know what to put on it," he said. Anyone breaking into Citicorp's electronic mail, he said, would find information of "only minimal" business value.

Even less clear than the law on breaking into an electronic mail system are the legal standards for access by law enforcement officials. For investigators, electronic mail records could be an extremely valuable source of information. "Electronic mail is tremendously attractive to people who are engaged in investigations," said attorney Plesser. "I think law enforcement officials are going to be-

come more and more interested in electronic mail records."

Certainly electronic mail networks will contain a wealth of data about the communications of their users. Telenet holds in its computers for anywhere from one day to two weeks copies of messages sent through the system. MCI plans to hold copies of the messages for six months, in case questions arise about billing or customers accidentally erase their messages.

Just the fact that MCI's computer capacity will enable it to hold the messages it transmits for six months makes "some customers nervous," said Marilyn M. Mouly, vice president for marketing of MCI Digital Information Services Corp., the subsidiary that runs MCI's electronic mail system. "When you mail a letter with the Post Office, they don't Xerox it. Generally people see us as carrying messages, not keeping a copy."

There are clear rules on when ordinary mail sent through the Postal Service can be opened. Most correspondence can be opened only after a search warrant is obtained. When law enforcement officials want the Postal Service to tell them from whom a specific individual is receiving mail, they request a mail cover from the chief postal inspector. Under regulation, the inspector is supposed to approve requests only for the investigation of a felony, the location of a fugitive or a national security investigation. In 1983, the Postal Service approved 6,892 mail covers, up 56 per cent from a decade ago. Postal Service officials say these same rules would apply to mail sent through the Postal Service's electronic mail system, known as E-COM.

But the rules for access to privately transmitted electronic mail have not been established. "There is little, if any, legal protection for message information in the hands of private organizations," said Rand Corp. computer security expert Willis H. Ware in recent congressional testimony. In an interview, Ware said he was aware of no law that would prevent a private firm from releasing electronic mail records to police agencies—or anyone else—merely upon their request.

Both Telenet and MCI said they would not release the information to law enforcement officials on request alone and would require a search warrant or a subpoena. But those are voluntary decisions subject to change, and some in the industry would like to see clear legal standards. "It certainly is a gray area of what kind of protection a company has from federal government intrusion," said computer consultant Ulrich.

Similarly, there are no laws governing requests by police officials for the records of the traditional courier services, such as Federal Express. Federal Express author-



Ronald L. Plesser, former general counsel of the Privacy Protection Study Commission: "Our laws have not kept pace with the [new computer or communications] technology."

ney Elizabeth McKanna said the firm generally would require a subpoena before releasing records, but in some cases, such as the investigation of a bank robbery, might not. "It certainly is not illegal for us to provide them with information," she said.

ELECTRONIC BLINDSPOT?

Also in dispute among experts in the field is whether any law protects an electronic mail transmission or any other communication between two computers, from unauthorized interception while it is in transit.

Two laws govern the interception of telecommunications. Title III of the 1968 Omnibus Crime Control and Safe Streets Act bans the private interception of wire or spoken communications and establishes a process for approval of wiretaps by law enforcement officials. To wiretap a suspect, a federal law enforcement official must obtain the approval of the Attorney General and then a federal judge after demonstrating that there is "probable cause" that the suspect has committed or is about to commit one of a list of specified crimes. Approval is granted only for 30 days or less, and the law allows the judge to require reports on the investigation. These standards are much tougher than the rules governing search warrants or other investigative tools. The second law, the 1934 Communications Act, makes it illegal "to intercept any radio communication and divulge or publish" the contents.

The problem for computer communications arises from the definition of intercept in the crime control law. Though it bans unauthorized interception, the law defines that as "aural acquisition of the contents of any wire or oral communication"—that is, the interception of a voice communication that could be understood by the human ear, as a wiretapper listening to an ordinary phone call would do. But computers utilize non-aural communications that transmit data through a series of digitized bits that cannot be understood by the human ear. For that reason, they are not covered by the law.

No one is accusing the Justice Department or FBI of abusing this provision of the law. Deputy assistant attorney general for the Criminal Division John C. Keeny said in an interview that he has not seen any requests to intercept computer transmissions. But computer users and civil libertarians are concerned that the potential for abuse remains unless computer transmissions are given the same legal protections as telephone conversations.

G. Robert Blakey, a law professor at the University of Notre Dame, who was the principal author of Title III and several other major crime bills when he was an aide on the Senate Judiciary Committee, said that the exclusion of computer communications was not an oversight. "Did we intend to exclude machine-based data? Yes we did," he said in an interview. Congress was worried about wiretaps, whose use had been severely limited by two Supreme Court decisions in the mid-1960s, not about computer privacy, Blakey said. "Congress wasn't prepared to step into computer privacy, and that's the reason we put that word [aural] in there," he said. "Aural" is a neat little word. It simply confines the bill to the consensus that was there" in Congress at the time.

The Justice Department agrees that computers are not covered and that federal officials would not have to go through the extended Title III process to intercept communications between two computers. In a 1978 case, *U.S. v. Seidman*, the U.S. Court of Appeals for the 4th Circuit also ruled that non-aural communications were not protected by Title III.

That much seems clear. What is unclear is whether law enforcement officials have to go through any legal process before intercepting computer transmissions.

One answer comes from the courts' rulings on pen registers, devices that record the numbers dialed on a phone, but not the contents of the conversations themselves. In the mid-1970s, American Telephone & Telegraph Co. (AT&T) asserted that the FBI had to receive a Title

III authorization before the company would install pen registers. The FBI argued that an ordinary search warrant was sufficient. In December 1977, a sharply divided Supreme Court ruled, 5-4, that because the pen register was intercepting non-aural communications (the tones that indicate the number dialed) and legislative history made clear Congress intended to exclude pen registers, the FBI did not need a Title III warrant. In two subsequent cases, the Supreme Court and a federal appeals court have held that law enforcement officials did not even need a search warrant to install a pen register. Nonetheless, H. W. William Caming, AT&T's senior counsel on privacy issues, said the firm will not cooperate with pen register requests without a warrant.

But the signals captured by pen registers may be different from other computer transmissions. Because the caller knows that records of the numbers he dials will routinely be held by the phone company for billing purposes, he does not have the same expectation of privacy for that information as he does for the contents of his conversation.

In a transmission of information between two computers, though, the parties would have a reasonable expectation of privacy, several experts said. Legally that expectation puts the communication under the 4th Amendment's protection against unreasonable search and seizure, these experts argue. "In a computer-to-computer transmission, there is a reasonable expectation of privacy, and any interception would be violative of a person's civil rights if done by law enforcement officials without a search warrant," said Caming.

Moreover, a Senate expert on surveillance maintained that the 1978 Foreign Intelligence Surveillance Act, which covers national security wiretaps on foreign agents, limits the ability of federal law enforcement officials to tap non-aural communications. One section of the foreign intelligence law prohibits any federal wiretapping not specifically authorized by statute, he argued, and Title III, because it does not mention non-aural interception, does not specifically authorize it. The foreign intelligence law provides a defense against that ban if law enforcement officials have obtained a court order or search warrant. Other experts, such as Caming, dispute that interpretation of the foreign intelligence law and maintain that it has no bearing on domestic wiretaps.

Justice Department official Keeney said that "if you are going to make any sort of invasion or intrusion, get a court order." It would be his "guess," he said, that law enforcement officials seeking to



Marilyn M. Mouly of the subsidiary that runs MCI's electronic mail system says the fact that MCI's computer capacity will enable it to hold messages it transmits for six months makes "some customers nervous"

intercept computer transmissions would not necessarily need a search warrant—which requires probable cause—but a court order, for which they would have to meet a lesser standard of proof.

But Keeney said he could not make a blanket statement that all interceptions of computer transmissions would require even a court order. "I'm not ready to go that far, no," he said. "You're dealing with a question of expectation of privacy. In some of these areas, there is no expectation of privacy. If you're putting something in the airwaves that almost anyone can pick up, there is no expectation of privacy."

PRIVATE WIRETAPPING

The same kind of uncertainties arise over the laws prohibiting the private interception of computer transmissions. Again, it is clear that Title III's ban on private wiretapping does not protect computer communications, since they are non-aural. But does any other law apply?

Many experts are concerned that there are no clear federal laws prohibiting the private interception of computer transmissions. Other laws could be stretched to cover that situation, said AT&T's Caming: someone intercepting computer transmissions might be prosecuted under the federal wire fraud laws, or under computer protection statutes in the states that have them, and could even face civil liability for the theft of trade secrets. "But," he said, "that is not as strong a deterrent as a specific federal law."

An attorney for a private data transmission company said that the 1934 Communications Act, which bars the unauthorized interception of radio commu-

nications, could protect some of these messages. Before 1968, this law had established the rules for interception of both wire and radio communications, but Congress removed wire communications from its scope with the passage of the crime control act.

Computer messages, though, like other telecommunications, often go through several steps to completion: along local phone wires, through microwave relays and off satellites. The attorney argued that the 1934 act's ban on intercepting radio communications would make it illegal to intercept computer communications during the microwave or satellite, though not the wire, portions of their journey.

At least two appellate court decisions cast doubt on that interpretation. In a 1973 case, the U.S. Court of Appeals for the 9th Circuit ruled that when any part of a communication is carried by telephone wires, the entire communication is covered not by the Communications Act but by Title III. In a 1975 case, the U.S. Court of Appeals for the 5th Circuit rejected the argument that long-distance calls carried over microwave relays were covered by the Communications Act.

AT&T's view, said Caming, is that both the microwave and satellite portions of a telephone communication fall under Title III's definition of a wire communication.

Blakey, though, argues that it is erroneous to assume that courts would come to these same conclusions about the coverage of the Communications Act if faced with a private interception of computer transmissions. In defining wire and radio communications, the courts have gener-

ally been looking for ways to allow evidence obtained by law enforcement officials to be used over the objections of defendants who maintain that it was illegally collected. It is not likely, Blakey maintained, that the courts would allow

it costs more to send an encrypted message. Citicorp uses a simple encryption for its electronic mail and a much more sophisticated system for its electronic funds transfers, whose security is of far greater concern to the bank. Those trans-

security payment records to uncover payments to people who have died.

In one case, during the final months of the Carter Administration, a regional HHS office in Sacramento analyzed its enforcement records to compile a portrait of what it called a "welfare queen" and then ran that profile against a list of county welfare recipients. Those who met the characteristics were singled out for further investigation, though because of staff limits, the office actually investigated only a few of those identified.

Over all, an HHS official estimated, the federal government has undertaken 2,000-3,000 matches, many of which are repeated regularly.

Supporters say that matching is a cost-effective and efficient way to uncover possible fraud in federal programs without creating an undue invasion of privacy. "Of course we have to match," said former privacy commission chairman Linowes. "You have a need for law enforcement, for proper administration in government. You just can't say one thing is completely wrong in most cases."

Critics say that even if each individual use can be justified, the cumulative uses of computer matching can constitute a serious invasion of privacy. Public opposition quickly grounded plans discussed by the Johnson Administration to create a national data bank that would have centralized all the data held on individuals by the government. Matching, said John H. Shattuck, national legislative director of the American Civil Liberties Union (ACLU), accomplishes the same end "through the back door."

Some critics say that matching undermines 4th Amendment protections, since the records of all individuals in a program are searched, not only those for whom program administrators have reason to suspect of a crime. Others, such as Sen. William S. Cohen, R-Maine, worry that in the rush to find waste and fraud, the privacy implications of the growing use of matching are being overlooked.

"As you look at each case, you can make a reasonable case for an exemption from our privacy law," Cohen said in an interview. "I'm trying to say we need to stand back and take a broader view. ... There is another pressure [besides looking for fraud], more constitutional, more indignant to our society, which is not being felt at this time: the need to protect privacy in our technological society."

The Massachusetts case demonstrates both the advantages and hazards of matching. In one instance, the state terminated the medicare benefits of an elderly woman in a nursing home because she possessed assets over the limit. But it was later revealed that her major holding

Computer users and civil libertarians are concerned there is potential for abuse unless computer transmissions are given the same legal protections as telephone conversations.

private wiretappers to use those definitions to slip through a blind spot in the law and escape punishment. Wiretappers would face liability under either the wire fraud statute or the Communications Act, he said.

Nonetheless, Blakey, like many other experts in this area, said he would "applaud any effort by Congress to take a look at the specific protections" available for computer communications. Several legislators already are. Kastenmeier's staff has been looking at the issue, and Sen. Walter D. Huddleston, D-Ky., a member of the Select Committee on Intelligence, has indicated he would support legislation to protect non-aural communications.

Whatever the state of the law, catching private wiretappers is not easy. No one has a good estimate of the amount of private wiretapping that is going on, said computer security expert Ware.

Although it is technically easy to intercept microwave transmissions, most would-be wiretappers are deterred from seeking to tap the phone company's network that way because of the high cost of sifting through the mass of messages flowing through the microwave links to find the ones they want. (That is not a problem if the wiretapper is looking for the messages of a single company, such as Citicorp, that are carried along a private network.) Usually private wiretappers seek to intercept messages by breaking into local phone lines near the subject, say security experts.

The Carter Administration, which was concerned about the Soviet Union's intercepting microwave transmissions with equipment in its offices in New York, San Francisco and Washington, undertook a series of steps to increase the security of government communications and pushed private companies to protect their communications through encryption, or encoding of the information. Only about 100 companies, mainly financial institutions worried about embezzlers sending phony messages to transfer funds, encrypt their data communications, said a government official.

Firms have resisted encryption because

fers cost twice as much to send as the electronic mail messages.

To some extent, new telecommunications technology itself will offer greater protection against interception. More messages are being sent through packet switching technology, which breaks up a communication into separate pieces and routes each piece along whatever space is free on many different communications paths. The result is that a single message may travel on several different paths, and the bits of information following each other on any single path may be unrelated.

AT&T is changing its current system under which a phone conversation follows on the same communications path as the tones that indicate which phone number has been dialed. That system allows wiretappers to program their computers to look for a specific phone number and then begin recording. Under the new system, which is already in place in half of the interstate network, the tones will travel along a different path from the communication itself. Neither of these offer insurmountable problems to the most sophisticated wiretappers—such as the Soviet Union—but they do make the job harder, communications experts say.

COMPUTER MATCHING

Another area where privacy laws are fuzzy is the use of computer matching, a technique used by government investigators to find fraud. Matching takes many forms, but generally it entails the computer comparison of two lists to find anomalies that would indicate fraud.

In Massachusetts, for example, state welfare officials have compared recipient roles for welfare, medicare, food stamps and other benefit programs against account records in the state's banks to find beneficiaries with more than the legal limit in assets. The Health and Human Services Department (HHS) has matched welfare rolls against lists of federal employees and compared the employee lists with the list of those who have defaulted on student loans. The department's Project Spectre compares medicare and medicare death files to social

was a funeral bond, which is permitted under the rules. Since then, the state has made procedural changes in the match program that have alleviated many of the concerns of advocates for benefit recipients. And the state estimates it has saved at least \$5 million by finding 2,000 benefit recipients with assets over the legal limit.

The law governing the use of federal records is the 1974 Privacy Act. The act generally prohibits the dissemination of government records outside of the agency that collected them. But because of a concession made to get the bill through, the law allows agencies to exchange records for "routine use." That is defined as a purpose "compatible" with the one for which the records were originally collected.

The routine use exemption has become the legal basis for matching. Matching critics say that the intent of the privacy law was to prevent records from being passed between government agencies on a regular basis. "I don't think there was anything more clearly thought about than that," said James H. Davidson, a former Senate aide who helped draft the law. "That is what the Privacy Act is about." When the Carter Administration proposed its first match of federal employees against welfare rolls, the Civil Service Commission initially resisted on the ground that such use of employment records would violate the act.

But eventually, the commission backed down. And Shattuck said that whatever the intent of the Privacy Act's drafters, the language of the statute makes it virtually impossible to challenge a match in court. "I think any match that uses information that is not clearly in the public domain is a violation of the Privacy Act," he said. "Unfortunately, the act is written in such a way as to make that extremely difficult to prove in a court of law."

Christopher C. DeMuth, administrator of the Office of Management and Budget's (OMB) office of information and regulatory affairs, which is charged with ensuring federal compliance with the Privacy Act, agreed that the law does not offer clear guidance on what matches might be inappropriate. Congress, he said, "had to settle for a formulation that is sometimes attacked as too nebulous." But he said the fears about matching have proven unfounded. "The fears that these matches would be used as fishing expeditions have not come to pass," he said in an interview. "The matches have been quite narrow and related to highly plausible concerns about fraud and abuse."

With budget cuts forcing welfare program administrators to trim benefit rolls, few legislators have expressed much con-



Sen. William S. Cohen says there is a "need to protect privacy in our technological society."

cern about the privacy implications of matching. The House Government Operations Committee recently criticized OMB for not monitoring agency compliance with the Privacy Act. Cohen held hearings in December 1982 on matching and is planning hearings on matches conducted by the Internal Revenue Service, including the use of mailing lists purchased from private firms to look for tax evaders and the growing use of IRS data for nontax purposes such as aiding in the collection of student loans. Recently, the National Senior Citizens Law Center won a case in the U.S. District Court for the District of Columbia stopping a proposed Social Security Administration program that would have required recipients of supplemental security income benefits to disclose their tax returns.

But over all, said Cohen, there is "not a whole lot of interest" in the subject among his colleagues. "The potential for abuse is there," he said, "although it does not seem imminent to most individuals."

That assessment does not surprise Robert Ellis Smith, who has been watching these issues for almost a decade as publisher of the *Privacy Journal*. "I think legislation often gets enacted by anecdote," he said. "And the anecdotes are often more compelling on the side of access."

CONTROLLING RECORDS

For records held by the federal government, the Privacy Act establishes minimum standards that allow individuals to

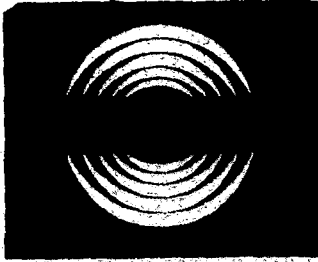
see and correct their own records. But for the vast majority of records held by private firms, there are no laws. Congress has passed legislation placing some limits on the use of records held by banks, credit bureaus and educational institutions. And last year, as part of cable television legislation, the Senate voted to limit the use of information about subscribers without their consent. Similar provisions are contained in the House version of the bill, which has passed the House Energy and Commerce Subcommittee on Telecommunications, Consumer Protection and Finance. In full committee, it is likely that efforts will be made to revise those standards to reflect objections from the cable industry and advertisers who sell products on cable.

But generally, Congress has paid little attention to the central thrust of the privacy commission's study in the mid-1970s. The commission argued that basic principles were needed to govern data collection and use of information about individuals held by institutions and to ensure that individuals could see and correct information about themselves. Since that report, only the legislation governing bank records, which is considered weak by many privacy experts, was enacted. Another major proposal dealing with medical records failed.

Like the issues of electronic mail and protection of computer transmissions, the use of privately held records has not yet attracted sustained political attention. "Our concepts involving information privacy haven't even begun to be addressed," said former privacy commission chairman Linowes. "We don't have a public policy on information protection and privacy."

Such a policy would not require limiting the advance of computer and communications technology. Linowes and other experts argue, but would establish principles of law. "The technology makes it easier both to collect and disseminate personal information without the person's knowledge," said Richard M. Neustadt, who worked on privacy issues as an associate director of the domestic policy staff in the Carter Administration and is now the senior vice president of Private Satellite Network Inc. "But that's nothing new. We've had personal records existing in file cabinets for a long, long time. All the computer does is put more records in and make it easier to get at."

"What we're seeing is old problems made more complicated, more real. But they are solvable. I think you can have your cake and eat it too, if we write some good rules about this stuff. Unfortunately, there doesn't seem to be much interest in doing that in Washington now." □



That's not a picture hook — it's a 'bug'

By Peter Grier
Staff writer of The Christian Science Monitor

Washington
One hundred eighty miles above the earth there soars an electronic eye so keen that eagles, by comparison, are blind as bats wearing sunglasses.

This marvel is the US KH-11 spy satellite, alias "Keyhole." The KH-11's cameras can pick out cars in the Pentagon

PART 1

parking lot — while the satellite is over, say, Detroit. They can see moving tanks in the dark, and are able to detect camouflage trees.

"US satellites are the best in the world," says a former military intelligence officer, arms waving with excitement as he discusses the subject. "Easily the best in the world."

They are also the cutting edge of a technology most Americans know little about: high-tech surveillance equipment. Over the last five years, microchips and miniaturization have led to tape machines that can record 40 conversations at once, tiny TV cameras that see in starlight, and "bugs" disguised as picture hooks.

One firm even predicts that camera-equipped computers will soon be able to recognize individual people.

These devices, for the most part, are intended for good use: catching crooks, plant protection, international intelligence-gathering. In many ways they make

our lives more secure.

Yet the very existence of these high-tech eyes and ears compels our vigilance — just in case — say those who study privacy subjects.

"We have all the technology [Orwell] anticipated," notes Robert Smith, publisher of Privacy Journal, "and more."

In fact, an amazing array of surveillance devices are available off the rack, like ready-to-wear suits. Others can be easily assembled from parts sold at many radio and drug stores.

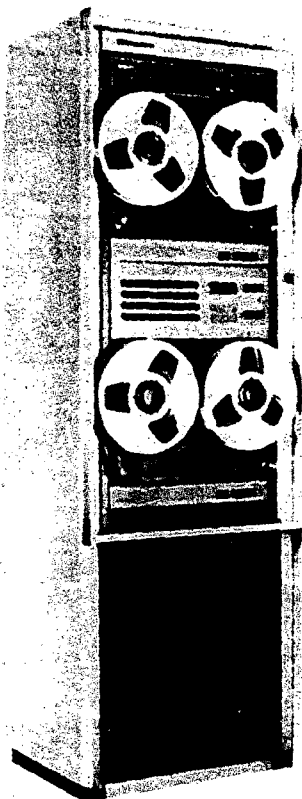
• The Dictaphone "Veritrac," sold mainly to law-enforcement agencies, is a refrigerator-size tape recorder capable of monitoring 40 phone calls at once. At the other end of the scale, CCS Communications of New York sells (in states where it's legal) a desktop humidor that contains a tiny, voice-activated recorder.

"There are microcassettes [recorders] advertised in the Wall Street Journal that are vastly better than anything the government had five years ago," claims an electrical engineer who has worked with intelligence agencies. "They fit right in your palm. They don't even stick out beyond your fingers."

• Video cameras the size of a deck of cards will be available this spring from RCA Corporation. In place of bulky image tubes, these tiny eyes use slices of photosensitive silicon. Cameras currently on the market can already "see" by starlight and transmit pictures by microwave.

• Motion sensors that use infrared or ultrasonic waves, once limited to space shots and expensive weapons, have become standard items in the catalogs of such security firms as ADT and Bocal. They are used in spots where normal cameras are useless: The National Park Service, for instance, has used infrared sensors in the recent past to count hikers in heavy forest foliage.

• Advanced technology has rendered the "bug" planted by the Watergate burglars as obsolete as a phone made from tin cans and string. Mix together the microphone from a hearing aid, a pared-down



'Veritrac' monitors 40 phone calls at once

watch battery, and a few odds and ends, and you can today produce an illegal listening device the size of a picture hook.

"They only work a few hours or days, but you can't even recognize them as bugs," says Harry Augenblick, head of Microlab/FXR, a company that makes bug detection devices.

Furthermore, surveillance gadgets today are often linked together in security systems, then turbocharged with add-on electronics. This extra power gives the systems a smattering of "intelligence." RCA's digital motion detector, for instance, enables cameras to distinguish between a guard on routine rounds and someone entering a restricted area.

Advances in computer technology will eventually make security systems even more discerning.

"Now there are special computers being designed that will be able to recognize people," says Harold Krall, an RCA vice-president of the closed circuit video equipment division. "This whole industry is in tremendous ferment."

Of course, equipment sold at the corner security store is crude and bulky compared with the high-tech eyes and ears used by the United States government. "Q," the disheveled gadgeteer who makes James Bond's espionage knickknacks, has little imagination compared with the scientists who work for the Pentagon.

US intelligence agencies, for instance, have in the past trained pigeons to deposit bugs on windowsills, according to congressional documents. They have experimented with microwave lie detectors that measure stomach flutters from half a mile away. Eavesdropping lasers, which work by "listening" to windowpane vibrations, are reportedly standard Central Intelligence Agency (CIA) fare.

But the Mercedes of surveillance devices is undoubtedly the US spy satellite. The most advanced US skyborne eye, the KH-11, orbits the earth at an altitude of 160 to 180 miles, snapping away with both enhanced-color and infrared cameras, according to intelligence and scientific sources. Photos are either beamed straight back to earth or dropped overboard in parachute capsules.

Its multicamera capability allows the Keyhole to see in the dark and strip away camouflage. The satellite can focus on objects as small as a Toyota — but it can't yet pick out lettering on crates, or tell Cuban advisers from Nicaraguans.

"A lot of the stuff you hear [about the KH-11], reading license plates and things

like that, is exaggerated," says one knowledgeable source.

Other surreptitious US satellites include the KH-9, which scuds along in a low orbit for clearer pictures, and the Rhyolite, which eavesdrops on radio transmissions from its parking spot 22,000 miles above the Earth.

The purpose of all this electronic gear is to spy on foreign nations, so the US can know better what's going on in the world. There is evidence, however, that these satellites have in the past turned and focused on Americans.

A CIA memo of May 8, 1973, written by then-Deputy Director Edward Proctor, implies that the US government spied on domestic demonstrations from space. The memo, obtained by the Center for National Security Studies and read by this reporter, says that the agency's satellite photo arm "has examined domestic coverage for special purposes such as natural catastrophes and civil disturbances."

In addition, Dow Chemical in 1980 accused the US of using satellite photos to monitor pollution from factories.

This sort of evidence leads to the larger issue of control of surveillance technologies. Should we worry about the advent of 40-track tape recorders and fist-size TV cameras? Once computers have been trained to recognize people, will they someday be programmed to search for us?

The advent of computerized information networks — automatic teller systems, electronic mail — makes this question of control of technology more urgent.

"Technology can create new opportunities for privacy invasion, manipulation, and control," concludes an Academy of Political Science privacy paper, "but it does not by itself create the structure of power that commits those abuses."

Notes Anthony Gettinger, head of the Harvard Center for Information Policy Research: "The problem with the metaphor of Big Brother is that it suggests some kind of outrageous dictatorial power [is out there]. Reality is much more subtle than that."

First of six articles. Next: electronic eavesdropping.

APRIL 17, 1984

Who's snooping and how?

US and USSR 'peer into mist'

By Peter Geler
 Staff writer of The Christian Science Monitor

Washington

Pretending to be a Soviet eavesdropper, I peer into the purple mists of northern Virginia, searching for the octagon.

I am standing on the roof of an apartment on upper Wisconsin Avenue, one of the highest spots in Washington. Next door, the spindly legged frame of the new Soviet embassy is just emerging from morning shadows.

From this vantage point, two things about the half-finished embassy quickly become apparent: 1. The Soviets will have a great view. 2. Their antennas will pick up more than HBO and "This Week with David Brinkley."

To the south, next to the gray ribbon of I-395, the Pentagon is clearly visible. To the east is American Telephone & Telegraph's (AT&T) Arlington switching station, which sends an electronic beam of phone calls hooting right over the Soviet site. A few blocks north are the towers of the Naval Security Station and Western Union's Tenleytown microwave relay.

The prospect of foreign serials in the midst of this electronic interchange illustrates a dilemma of modern telecommunications. Whiz-bang technology makes the United States system the best in the world, say electrocommunication experts — but that same technology makes it relatively easy to intercept messages.

The USSR, from trawlers, trucks, and rooftops, has been listening in on our phone calls for years, say US officials with access to intelligence information.

The National Security Agency, the US government's secretive electronic intelligence arm, scans an unknown amount of US messages headed overseas, according to court records and civil liberties advocates.

Furthermore, it may be perfectly legal for anyone to eavesdrop on computer communications. Experts worry that wiretap law may cover only human speech, leaving the "beep-de-beep" of computer talk unprotected.

In general, it is the demise of the wire which has made these activities possible. Once, phone calls traveled only paths of copper; today many are shot across country by microwave. Microwave beams can be a third of a mile across, and to catch them, all an eavesdropper must do is hoist small dish antennas in their path. If the beam is an AT&T trunk line, sophisticated computer analysis is then required to unravel it.

Overseas messages bounced off satellites are even easier to grab. With a good dish, satellite traffic can be stolen from anywhere in the US, from ships offshore, "even from Cuba," wryly notes a former White House communications official.

Wireless phones are vulnerable, too. If you have a cheap model, neighbors may be able to hear parts of your conversation on AM radio. Last December, police in Woonsocket, R.I., used this eavesdrop technique to snare a 19-member drug ring.

All this doesn't mean there are lots of little guys out there listening to your calls. For the most part, only nations indulge in extensive electronic eavesdropping.

The Soviet Union is the most notorious example. Their buildings — from the old Embassy on 16th Street here, to the United Nations Mission on 67th Street in New York, to the West Coast consulate on top of a San Francisco hill — are topped with forests of antennas. From these rooftops and elsewhere, the USSR has been listening in on US phone calls for at least a decade, say government and academic sources.

They are probably after more than military secrets. "Department of Defense (communications) will be encrypted," says an official who worked on the issue for the Carter administration. "The problem is that sensitive private-sector information is vulnerable."

Conversations pulled from the sky have likely helped the Soviets in grain-contract negotiations, for instance, says this source. Their Glen Cove, N.Y., weekend lodge is well-positioned to listen in on Long Island's defense industries. The San Francisco consulate is thought to hide equipment trained on Silicon Valley.

Defensive measures have been taken since the eavesdropping was first discovered. US government communications have been rerouted underground; important defense contractors have been outfitted with government scramblers. AT&T now beams most microwaves in a way that is much more difficult to unravel, says Willis Ware, a Rand Corporation communications expert.

But the USSR, at the same time, has been updating its interception gadgets. Overall, "the situation is more or less the same," claims a congressional aide with access to intelligence information.

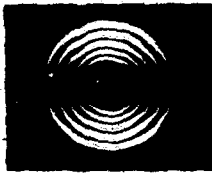
Other nations probably have electronic eavesdropping equipment in the US, though not on the same scale as the Russians. The US itself, however, has high-tech ears that put the Soviets to shame.

The National Security Agency (NSA), the US electronic intelligence arm, has six times the number of employees of the Central Intelligence Agency (CIA), according to congressional estimates, and has giant antennas from suburban Washington to Pine Gap, Australia.

Most of these ears are trained on other nations, straining to pick up chatter between Soviet pilots or data from Chinese missiles. But some are turned inward to monitor US phone calls and telegrams headed for other nations.

NSA dishes in Sugar Grove, W.Va., can eavesdrop on a nearby COMSAT post that handles half of all US international satellite communications, says James Bamford in his book "Puzzle Palace." NSA installations in Maine, Washington State, and California have similar purposes, he claims.

The NSA sweeps up vast numbers of messages headed overseas from the US, according to records from a 1982 court case on use of the agency's intelligence. High-speed computers then rifle through this raw data at



PART TWO

leisure. When they stumble across a keyword ("Khomeini," perhaps) that means the message might be useful, it is printed out for further study. Other communications are discarded.

A US appeals court judge, in the context of the '82 suit, did not find this activity illegal. But some congressional aides and civil libertarians feel the NSA impinges on citizens' constitutional rights, as the agency's methods inadvertently filter millions of innocent messages.

"The intrusion is no less serious because it's so quick, or because no trace is left, or because no human is involved," says David Waters, an electrical engineer and former consultant to the CIA.

The NSA's power has been abused in the past: Between 1945 and 1976, under "Operation Shamrock," the agency was given copies of almost all telegrams sent overseas. During the Vietnam war era, the NSA listened to conversations of Jane Fonda, Dr. Benjamin Spock, and others on a "watch list" of 1,650 protesters.

Today, "the NSA does not target the communications of US citizens," a former NSA director, Vice-Adm. Bobby Inman, said in an interview.

"The provisions are also in place to suppress any potential for saving a 'watchlist' of knowledge that's incidentally acquired," he added. "There is not, in fact, a

danger of Big Brother turning to listen to the communications of its citizens."

There may be a danger in the US, however, of unwanted ears listening in on the communications of computers. The 1968 Crime Control Act, which governs non-national-security wiretaps, prohibits "aural acquisition" of telecommunications. In other words, it's illegal to intercept a communication you can hear and understand.

But as anybody who's ever listened to computer "speech" knows, you can hear it — but you can't understand it.

Ron Plesser, counsel to the 1977 Privacy Protection Commission, says that means that it may be perfectly legal to eavesdrop on computers. "It's a real issue," he says, "although I don't think it's that hard to fix."

This glitch is a good example of how quick-footed innovation often outflanks efforts to control and protect it.

"These technological advances happen so quickly that the normal process our government and society uses for adjusting to change doesn't have time to take effect," says Arthur Bushkin, a former Commerce Department information policy official.

Second of six articles. Next: domestic wiretapping.

Inman: little chance of intentional domestic spying

Washington
Bobby Ray Inman doesn't look like a spy. With his prominent glasses and equally prominent grin, he could be a copier salesman or the owner of a string of convenience stores.

But the Rhomboro, Texas, native in fact is one of the premier United States intelligence officers of the post-World War II era. Among other things, Mr. Inman, a retired vice-admiral, has been director of naval intelligence, vice-director of the Defense Intelligence Agency, chief of the National Security Agency (NSA), and deputy director of the Central Intelligence Agency (CIA).

"This country does need to have strong, healthy, viable intelligence organizations," insists Inman, now head of MCC Corporation, a microelectronics research company.

For the most part, the US public supports this goal, he says — with the caveat that spy agencies never again "resort to domestic surveillance," as they did through the Vietnam war.

The abuses of the past — CIA spying on antiwar protesters, NSA perusal of US telegrams headed overseas — weren't entirely the fault of espionage agencies, says Inman. "These weren't things the intelligence agencies decided. Gee, wouldn't that be great to do? They all flow from decisions at senior levels of the executive branch, telling the intelligence community to do them," he says.



Bobby Ray Inman

Today there is little likelihood of another Operation Chaos (the illegal CIA domestic spying program) or Operation Shamrock, NSA's long-term scanning of US telegrams headed overseas, says Inman. But with the NSA's electronic ears sucking up information all over the world, "the prospect of incidental, unintentional acquisition of information on US individuals is a reality," he admits.

NSA procedures guard against abuse of this data, he says. When it is recognized that a message contains the identity of a US citizen, that identity is suppressed.

— P. G.

THE CHRISTIAN SCIENCE MONITOR

WEDNESDAY, APRIL 14, 1984

Wiretaps: is there enough supervision?

By Peter Geler

Staff writer of The Christian Science Monitor

Newspaper, N.Y.

"KEEP OUT" is penciled on the battered door. We knock before entering, to make sure no one's inside.

The room looks like a junior high school teachers' lounge. It is windowless, with aged chairs, a Cyclops eye of a clock, and a carpet that was once orange. Along one wall stretches a counter that would be perfect for eating lunch — if you moved all the tape recorders.

"I wouldn't let you in if they were listening," says Ray Perini, chief of the Suffolk County narcotics bureau.

This, in fact, is a wiretapping lounge. From here, Suffolk County detectives with headphones and Superscope recorders listen in on suspects' phone calls. It's amazing, they claim, how loose-lipped criminals can be.

"They say stuff like, 'You talk, my phone is tapped,'" says Mr. Perini.

After declining steadily through the late '70s, the use of wiretaps in law enforcement is again on the rise. In 1982 (the last full year for which data is available) court-approved taps were up 22 percent, to 578. Preliminary figures show the numbers continued to climb during last year.

Yet wiretaps and bugs are powerful, potentially dangerous tools. The average tap hears 58 people, both guilty and innocent. "Videotapping" with tiny cameras can leave no place to hide.

Are investigators with headphones trampling on constitutional rights?



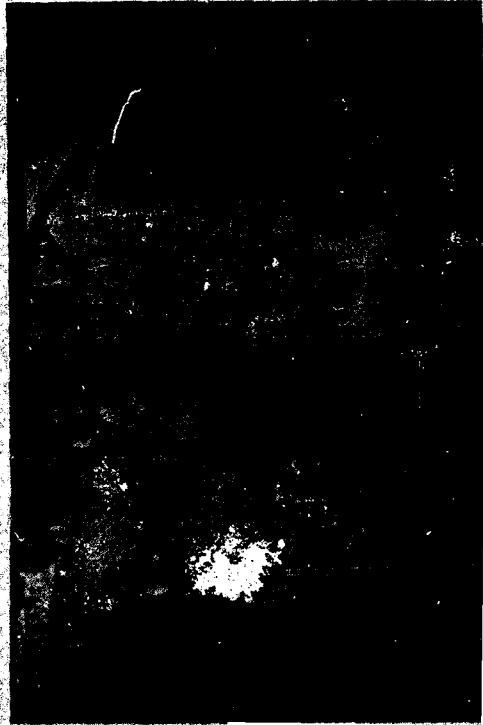
PART THREE

But to officials who use it often, electronic eavesdropping is an invaluable weapon in the war against crime.

Take the Federal Bureau of Investigation. Most of the jump in eavesdropping has been caused by the FBI, in its pursuit of drug rings. Fighting the new wave of such

"Wiretap law is a disaster," claims John Shattuck, national legal director of the American Civil Liberties Union (ACLU).

Over 50 years ago, United States Supreme Court Justice Oliver Wendell Holmes called police wiretapping a "dirty business." Even today, 23 states forbid their police departments from using taps and bugs.



Wiretap detection device

criminal enterprises, says FBI chief William Webster, requires greater use of "sensitive" techniques.

"I feel very comfortable using wiretaps, if guidelines are carefully supervised," Mr. Webster said in a recent interview. "They have been enormously effective. There's still a kind of carelessness where telephones are concerned."

In Suffolk County, on the eastern half of Long Island, there are apparently a lot of careless criminals.

Suffolk prosecutors installed more wiretaps in 1982 — 30 of them — than any other US county. According to federal records, about one-third of the 595 conversations these taps intercepted were "incriminating."

"You know that scene in the movie 'Annie Hall,' where Woody Allen sneezes and blows \$2,000 worth of cocaine all over the floor?" says Dave Freundlich, Suffolk assistant district attorney. "I heard that really happen once."

Often, says Mr. Freundlich, suspects know they are being tapped, and try to disguise the nature of their conversations. But their codes are sometimes less than cryptic.

"One guy will say 'Bring me a tire. A whole tire,' says Freundlich, "and then the other will ask, 'Do you want the big tire, or the little one?'"

Long Island's ragged shoreline is a haven for drug smugglers, and narcotics suspects account for most of Suffolk's wiretaps.

Without electronic help, claim county prosecutors, their arrests would reach no higher than street dealers. With taps, they say, they are getting the top dealers in the county — such as Ronald DeConza, convicted in '82

of distributing cocaine.

Assistant district attorney Freundlich insists that Suffolk detectives strictly follow federal wiretap laws. But he admits that the taps are "a big drain on our resources."

Indeed, wiretaps are as expensive as a Mercedes sedan. The average cost of a tap (including both equipment and manpower) was \$34,000 in '82, according to the administrative office of the United States Courts.

And that, say critics, is a lot to spend for something they consider both a dangerous intrusion on privacy and unnecessary.

"They should yank them all," grumbles Herman Schwartz, a law professor at the American University.

Wiretap are powerful vacuums that suck in the words of both criminals and innocent phone users. Between 1971 and 1982, federal taps overheard some 260,000 people — the vast majority of them innocent of any wrongdoing. Officials must turn off their equipment if a chat is not suspicious. But even a few seconds of eavesdropping, say civil liberties advocates, constitutes an invasion of privacy.

"They are inherently intrusive. It's analogous to searching all the apartments in a building, on the grounds that one may have something in it," says the ACLU's Mr. Shattuck.

Wiretaps are also sometimes unconstitutional "fishing expeditions," say civil liberties advocates. Officials reason, "Let's put a wire on this nasty guy and get him for something," critics say.

On a less theoretical level, eavesdropping critics argue that the technique is simply ineffective — that prosecutors, after they cast their electronics net, haul in only a few small criminals.

Over the last five years, wiretaps have led to the conviction of an average 900 criminals annually. The majority of these are small-time gamblers and street dealers, says Herman Schwartz of American University.

"If I was a Mafia figure, I would make damn sure never to say anything incriminating over the phone," Shattuck adds.

And judges probably don't watch over wiretaps as



PHOTO BY AP/WIDEWORLD

More taps on phone lines

SPY from preceding page

closely as they should.

The courts are charged with making sure officers follow the wiretap standards set in the Omnibus Crime Act of 1968.

But "the truth is, on the state level, oversight is difficult to achieve," admits a law-enforcement official who asked not to be named. "How would you like to lead through hundreds of conversations?"

The technique of wiretapping itself has changed little in the years since the Omnibus Act was passed. "Wiretaps" still find the phone box near a suspect's home or apartment, take a short wire with clips on each end, and connect the tapped line with one running back to the prosecutor's office.

Detectives then spend eight-hour shifts in bored seclusion, waiting for the tapped phone to ring.

But technology, since 1968, has not been standing still. Officials now use some gadgets the law did not foresee, such as electronic "pen registers," which record numbers dialed, not conversations, allowing police to

discover a suspect's contacts.

"Vidiotapping," in which small cameras watch suspects, is a still-smaller, but particularly Orwellian new development not covered by the law, says one congressional aide.

If your phone is tapped, you can keep your mouth shut. But if there's a camera in your calling, there's nothing

"The truth is, on the state level, oversight [of wiretap standards] is difficult to achieve," admits a law-enforcement official.

you can do, short of hiding under the table. A federal district judge, in 1980, called vidiotapping "extraordinarily intrusive," although he did not throw out camera-obtained evidence.

The use of bugs and phone taps raises difficult questions about both the need for security and rights to privacy.

It is a subject fraught with tensions.

"Electronic surveillance is the only way to get the big guys," sums up Michael Goldsmith, counsel to the New York organized-crime task force, "but its use needs periodic review."

That's in a nutshell. Next: Impact of technology on privacy.

Automatic tellers, electronic mail raise privacy concerns

By Peter Guter

Staff writer of The Christian Science Monitor

Annapolis, Md.

I am 50 miles and one state away from home, and in desperate need of money for lunch.

After all, this antique Chesapeake Bay town is famous for seafood, as well as sailing. Packs of Naval Academy cadets pass in front of me, enjoying crab cakes, oysters, and steamed clams. Their white hats look like dinner plates worn at a rakish angle.

So I slip my bank card into an automatic teller on West Street (laid out in 1696). Instantly, my request for \$20 is beamed to Baltimore, where a bank computer realizes I'm an outsider. It throws my query to Dayton, Ohio. A computer "switch" in Dayton checks with my Washington-area bank, then tells Baltimore it's all right to give me money.

In 10 seconds, thanks to an electronic banking network, I have cash for a crab sandwich — and a computer in Dayton knows I have skipped out of the office on a sunny, early spring afternoon.

Today, magic webs of computers are rapidly easing many of life's little tasks: getting cash, shopping, sending messages. But at the same time, these webs are hauling in vast amounts of personal data on Americans.

We must keep a careful eye on the rise of automatic banking, electronic mail, and other systems, say experts, if our privacy is to remain protected.

"As a byproduct of the evolution of technology, we are developing a network of surveillance capability," says Arthur Bushkin, who was in charge of President Carter's privacy initiatives, "although it's not out of any malicious intent."

The institutions that run computerized transaction networks all pledge to fiercely guard their customers' data. Yet gray areas in the law, say congressional aides and communications lawyers, may make these actions legal.

• Your boss, spouse, or a credit agency could track your movements with the use of electronic banking records. No federal law bars banks from divulging



PART FOUR

this information to third parties.

• If you use electronic mail, law-enforcement officers might be able to read your messages without a warrant. Search warrants are needed to open letters carried by the United States Postal Service.

• Subscribers to two-way cable television may find that opinions they register are sold to, say, political parties, with their names attached. Currently, the only laws protecting two-way cable data are state statutes in Illinois, Wisconsin, California, and Connecticut.

Back at the dawn of the information age, when computers took up the floor space of a hockey rink, civil libertarians feared the coming of the Big Box — a giant computer compiling data on everyone in the US.

Instead, during the last 30 years little computers have

learned to chatter back and forth, over communications links of unbelievable sophistication.

This gift of speech has made possible computer networks that today handle such tasks as reserving plane seats and approving checks. Decentralized, fast, hungry for data, these webs are far more than mere automated clerks, say those who follow privacy issues.

"More information is being maintained on individuals. It's being more centralized. It is more accessible and available," says Ron Plesner, a Washington, D.C., lawyer who was counsel to the 1977 federal privacy commission.

Today, the computers that know the most about us are probably those that handle financial tasks: electronic tellers, credit-card checking machines, and check authorizers. Besides knowledge of how much money we have in the bank, these systems know where we are depositing our paycheck, or paying \$150 for clothes — at the very moment we're conducting the transaction.

And money computers will be even more knowledgeable in the years ahead, as networks grow and combine to provide more services. Soon, for instance, American Express cardholders will be able to charge calls on specially equipped AT&T phones; eventually "debit" cards are expected to link banks and retailers by automatically siphoning cash from our accounts as we make purchases.

"The computer can develop a data base on your preferences: He likes to shop at this store, etc.," says Art Bushkin, now a telecommunications consultant. "It has time data. You can program it to behave presumptively: The next time Bushkin appears within the computer's scope, print out a message for the FBI [Federal Bureau



Computers now check credit-card transactions

of Investigation]."

Bank officials react indignantly when asked whether they might show this data to outsiders. Most financial institutions have explicit policies on protecting the privacy of their depositors.

But it is only the institutions' good will that guards these secrets, say privacy experts. The laws protecting financial records are very limited, they claim. If the federal government asks to see your bank files, the 1978 Right to Financial Privacy Act requires that you be notified. If a private party asks for them, it's perfectly legal for the bank to hand over the data without saying a word.

And if you think such things never happen, remember that Bob Woodward and Carl Bernstein, in pursuit of the Watergate story for the Washington Post, found California lawyer Donald Segretti's credit card records to be a rich source of information.

A Congressional Office of Technology Assessment study concludes that the need "for more comprehensive electronic funds transfer privacy protection . . . are still largely unmet."

If anything, there may be even less legal protection for message transmission systems such as electronic mail.

The electronic-mail business, long more promise than performance, is just now shifting into second gear. Private firms did about \$40 million worth of business last year, and in September MCI Communications launched its ambitious MCI Mail service.

Yet these ethereal messages, which flit from computer screen to computer screen, are more vulnerable than old-fashioned letters in several respects.

For one thing, some clever users of home computers have managed to break into the networks. Last summer, a gang of Milwaukee teens repeatedly romped through GTE Corporation's Telenet system.

No law explicitly makes this illegal. "It's a very large gray area," says Walter Ulrich, a computer consultant and head of the Electronic Mail Association's privacy committee.

For another thing, both law officers and private third parties might be able to read your messages without your knowledge. MCI, GTE, and other electronic-mail companies all say they will staunchly defend their subscribers' privacy. No law, however, prevents them from voluntarily surrendering your mail.

"Chilling, isn't it?" says Mr. Ulrich.

But it is still another type of computerized network that may have the greatest potential for invading our privacy: two-way cable TV.

Such systems promise to bring a world of services into our family rooms, via color TV. Futurists have long predicted that we will eventually be able to bank, shop, and express our opinion over interactive cable channels.

If so, we will be entrusting cable companies with huge chunks of data about ourselves: buying and viewing habits, perhaps even political and social opinions.

"This sensitive personal information is a valuable commodity which cable companies can sell to . . . interested buyers in order to finance their corporate growth," charges John Shattuck, national legal director of the American Civil Liberties Union.

No federal statute covers the issue. Four states, however, have passed laws prohibiting cable firms from disseminating individualized data. Two more — New York and Maryland — are considering similar laws.

The industry is sensitive to the problem. Warner-Amex Cable, which operates the QUBE interactive system in seven cities, subscribes to a privacy code that was the model for several of the state statutes.

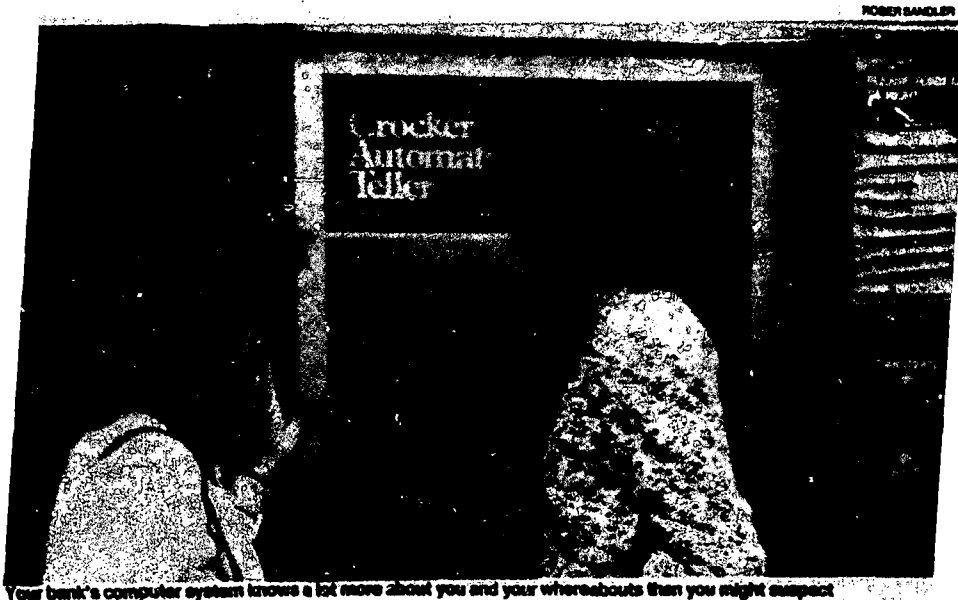
Of course, all these systems — two-way cable, electronic mail, and electronic banking — promise great benefits. Privacy experts say they simply want to see laws prohibiting misuse of the networks.

And "we should leave things flexible enough for the people who will want to continue the old ways," such as paying cash for gas, adds Robert Smith, editor of *Privacy Journal*.

Washington seems only mildly interested in the impact of computer systems on privacy. The House judiciary subcommittee on civil liberties, headed by Rep. Robert Kastanmeier (D) of Wisconsin is holding a series of hearings on the issue. The Commerce Department's National Telecommunications and Information Administration no longer works extensively on privacy.

"Do we as a society accept this evolution [of technology] and its implications passively?" asks communications consultant Bushkin. "Or do we discuss it and decide whether we like the way it is?"

Fourth in a series. Next: Encrypting computer data.



THE CHRISTIAN SCIENCE MONITOR

FRIDAY, APRIL 20, 1984

Computers now produce cipher as tough as 6-inch armor

By Peter Geler
Staff writer of The Christian Science Monitor

"DaX&N8e," says the secret message. "W@0y KlC:3" Sdfh."

Lapsing into a daydream, I wonder what it could possibly mean: Does McTavish know about the letters of credit, and the carpet dealer in Rabat? If so, then Diana is in danger. Why did the Land Rover have to break down? Cairo will be furious. . . .

Larry Conner of Analytics Communications, breaking my reverie, points to the computer screen in front of us.

"This word here is my last name, actually," he says.

We are in a sunny conference room, not a cheap North African hotel. I am being shown Sherlock, a black box that scrambles computer data into dense cipher. It is to paper-and-pencil code what a nuclear submarine is to a dinghy.

"The only known attack is to guess the key," says Thomas Mitchell, an Analytics marketing manager. "There are 72 quadrillion possible keys."

Cryptography — the science of secret communication — is entering a new age.

Gone are the romantic cipher machines of World War II, with their mysterious mechanisms; in their place are powerful microchips. And soon spies and diplomats may not be ciphering's main practitioners. As computer data becomes more valuable, cryptography is moving into the private sector.

"With electronic technology, you can have a much higher degree of security than with ordinary paper files in cabinets," claimed the late Kihai de Sola Pool, a communications expert at the Massachusetts Institute of Technology.

Take the Sherlock Information Security System. For \$1,200, it drapes secrecy over information transmitted

Roanoke, Va.

from one computer to another. Messages are unraveled with the aid of a "key," a 56-digit number, all 0s and 1s, which reverses Sherlock's scrambling equations.

Other ciphering equipment on the open market ranges from The Encryptor, an accessory for home computers that costs a few hundred dollars, to the IBM 3848. For \$58,670, the 3848 will encrypt just about anything.

"Say you've got one of our largest computers," says IBM spokesman Steve Carpenter, "and you wanted everything in it to be in ciphered. The 3848 could do it."

Of course, machines that make communications secret, as if by magic, have long fascinated ingenious inventors.



PART FIVE

In the mid-1400s, the Italian architect Leon Alberti perfected a cipher disk that was state-of-the-art technology for 400 years. Thomas Jefferson invented a "cypher wheel" which looked like a rolling pin and served the United States government for a century and a half.

By World War II, governments were encrypting with machines that resembled a cross between a typewriter and a music box. The machines, with such exotic names as "Purple" and "Enigma," used rotating electrified disks to scramble messages.

But with the rise of the digital computer, ENIGMA and its brothers were suddenly obsolete. Changing plain words into ciphertext is, at heart, a mathematical process; and computers do math so fast they produce cipher as tough as six-inch armor.

Computer technology, in fact, has reached the point where encryption equations now fit on a single microchip. The Data Encryption Standard (DES), a ciphering algorithm developed by the United States government, is available on chips made by Intel, Motorola, Texas Instruments, and many other makers.

These chips are the core of most private-sector encryption equipment. They do not produce impenetrable cipher, but just how much work it would take to un-

cover their secrets is a matter of some dispute.

A special state-of-the-art computer could crack open a DES-protected message in three days, according to a 1977 Stanford University study. The system's defenders claim such a computer is in fact wildly impractical, and that a more normal computer would need about 3,000 years to unravel a DES transmission.

In any case, DES provides enough protection for anyone short of a government, says Miles Smid, a mathematician with the US National Bureau of Standards.

"They make use of both substitution and transposition [scrambling] encryption," Mr. Smid says. "By using both types, you get a very strong cipher."

So far, commercial encryption is not exactly a hot trend. Analysts estimate that US sales of cipher devices hover between \$200-\$300 million a year.

But as computer networks proliferate and more companies become aware of the value of their electronically-stored data, demand is likely to see a healthy upswing, say communications experts.

"Everyone agrees that the market for cryptography will grow in the next 10 years. What is not clear is how much and how fast," a study by the Harvard Center for Information Policy concludes.

Banks will perhaps be the best customers for the "cryptosystems." Their computers, after all, are electronic vaults that literally store money.

Already, most financial institutions have encryption in their automatic teller machines, to protect customers' access numbers. Electronic funds-transfer (EFT) systems, which shuttle some \$600 billion between banks every day, aren't so well covered, since they're much more expensive to encrypt.

Howard Crumb, an assistant vice-president at the New York Federal Reserve, says only "parts" of banks' daily EFT transactions are in cipher.

"But I hear more and more talk about it," he says. "I see it coming on strong in late 1984. The catalyst was publicity about the 'hackers' who were breaking into computer systems last summer."

In the future, cryptology could also play a crucial role in protecting "information products" such as teletext and Home Box Office. The products would be broadcast in scrambled form; consumers would then purchase a key allowing them access to the data.

Many pay-TV channels already use such a system, points out Victor Walling of SRI International, a think tank in Menlo Park, Calif.

"The problem with a lot of these information products is that if you don't have a key to lock it up, you can't maintain rights to it," Mr. Walling says.

On the whole, however, Walling says there may not be a big private demand for cryptology, at least in the short run.

"Somebody will have to do a D. B. Cooper with data, before people will really pay attention," he says, referring to the legendary hijacker who parachuted from a Boeing 727 with \$200,000.

Meanwhile, science marches on. University researchers are hard at work on a new type of cipher that may make it even easier for businesses to transmit secret messages: "public key cryptology," or PKC.

Developed at Stanford and MIT, PKC uses two keys instead of one. The first can transform plain words into cipher, but can't decrypt the resulting message. The second, secret key is needed to unlock and read the transmission. Thus a subcontractor of a large oil company, by looking up the company's public key, could send it secret messages — but couldn't read the ciphered transmissions of a fellow subcontractor.

In addition, PKC allows users to add a unique digital "signature" to their transmissions. Eventually, business executives may legally be able to sign contracts by computer, say cryptologists, and exchange certified electronic mail.

Ronald Rivest of MIT, a PKC pioneer, says a computer chip featuring the new cipher will be ready by this fall. It will work more slowly than current encrypting chips, he admits. It thus may be most useful for such smaller applications as protecting information on certain credit cards.

Early versions of PKC have proved vulnerable to cryptologic attack. In 1982, a young Israeli mathematician, Adi Shamir, cracked a Stanford PKC system with relative ease.

But the PKC co-authored by Dr. Rivest, which uses more complicated calculations, has so far remained inviolate.

Fifth in a series. Next: Protecting privacy in a computer age.

Searching for privacy in a high-tech world: attitudes, not technology, are key

By Peter Grier
Staff writer of The Christian Science Monitor

Cambridge, Mass.

Congress in 1876 was in an uproar. The results of that year's presidential election were the subject of bitter dispute. Republican Rutherford B. Hayes and Democrat Samuel Tilden had finished in a virtual dead heat, with cries of fraud on both sides.

So legislators, to help settle the matter, decided to snoop on United States citizens via the latest in high technology — the telegraph. They simply ordered Western Union to turn over 30,000 telegrams from important political figures.

The press was aghast at this invasion of privacy. Western Union's president refused to comply. Congress arrested him

and read the telegrams anyway.

No conclusive proof of fraud was found. But the incident shows that "high tech" surveillance is not just a phenomenon of the 20th century. Throughout US history, experts say, the protection of privacy has depended on a mix of factors: technology, politics, and corporate attitudes.

"'Eternal vigilance is the price of liberty.' Some clichés gain currency and stay around, because they reflect basic truths," says Anthony Oettinger, head of Harvard's Center for Information Policy.

Speaking with the steady rhythm of a UPI ticker, Dr. Oettinger leans forward to



PART SIX

make his point. Outside, students scuffle across the Harvard Law School lawn.

The leader of a group whose sole purpose is studying the information revolution, Oettinger has "the whole wired world in his hand," according to Harvard magazine. He analyzes some 80 businesses — from cable television to newstands — for

their impact on the flow of data in the US. Microchip logic, tiny video eyes, and other new-tech gadgets could complicate efforts to shield privacy, he says. But he warns against focusing on the technology itself without scrutinizing society.

"There's no doubt some things are

done more efficiently with computers than with goose-quill pens. But I grew up in Europe in the '30s and '40s and saw many friends and relatives carted off by Germans using three-by-five cards," he says. "It doesn't require a computer."

Oettinger is obviously irritated by suggestions that surveillance technology, once born, creates a momentum of its own and will be used for nefarious purposes.

"That's like saying, 'Technology made me do it,'" he says, hands waving. "It's an absurd abdication of responsibility. There is no substitute for a free people, an electorate, whatever, remaining responsible and in charge. I mean, you've got to watch the [offenders], whoever they are."

This does not mean that evil forces

Please see PRIVACY page 24

PRIVACY from page 1

lurk just out of sight, ready to wrap the US in webs of surveillance the moment we let down our guard. Compared with both the fictional Oceania of George Orwell's "1984" and to many of today's totalitarian states, privacy in the US is well protected.

It does mean, Oettinger and other experts say, that we must watch for a step-by-step erosion of privacy by government agencies, corporations, and other institutions.

The benefits of new high-tech activities — from the use of computers to detect welfare fraud, to banking with electronic tellers, to on-line criminal information systems — should be weighed against possible intrusive effects.

"It's a balancing act," says Oettinger. "The balance is between privacy, an important value, and a lot of other things that we might want."

The US, since its founding, has officially prized privacy. The Fourth Amendment to the Constitution, for instance, guarantees the "right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures . . ."

But at the same time, US society professes admiration for those who have nothing to hide, for men and women whose lives are an open book.

"There is a stress on privacy in the US, and at the same time there is a stress on openness. That helps create a tension, I think, between concealment and revelation," says Sissela Bok, author of the book "Secrets."

Mrs. Bok, a Swedish-born philosopher, is the wife of Harvard president Derek Bok. Her father, economist Gunnar Myrdal, and her mother, peace activist Alva Myrdal, have both won Nobel Prizes.

Her elegant home is near Brattle Street in Cambridge. Outside the library, evening and a late-season snow are falling as she discusses privacy, technology, and secrets.

"With computers, we are in a whole new universe with respect to [protection of privacy]," she says. "In this uni-

verse we probably will have to recognize that there are a number of things that can't be exactly private."

The complexity of modern life, in other words, means that data we might prefer to keep private, such as bank balances and health records, won't be under our control.

And control, she says, is what privacy is all about — control over access to information we define as our personal domain. We thus guard our sense of identity.

"We recoil from those who would tap our telephones, read our letters, bug our rooms," Mrs. Bok writes. "No matter how little we have to hide, no matter how benevolent their intentions, we take such intrusions to be demeaning."

When our privacy is invaded, someone or something shows power over us. "If we had no privacy at all, not even the capacity to protect it with secrets, we would be utterly vulnerable," she says.

But privacy for people is not the issue that most concerns Mrs. Bok. Instead, she expresses concern about government secrecy.

The Reagan administration, she feels, has tried hard to slam shut doors to much information. It has become more difficult to pry loose documents through the Freedom of Information Act, she says; Presidential Directive 84, withdrawn after being blocked by Congress, would have required many officials to sign lifetime secrecy agreements.

"I feel very strongly that there has been a tremendous move towards greater official secrecy in many areas," she says.

Mrs. Bok says the US already has far too many secrets. She cites studies saying that many things labeled "top secret" are innocuous.

The light in the library is fading. Yes, Mrs. Bok concludes, there are technologies whose intrusive potential bears watching. Yet much information is still our own.

"Sometimes people, I think, assume in this country that there is little that is private anymore, little that is secret," she says. "There I just think they are wrong, actually."

Last in a series. Previous articles run April 16-20.



Sissela Bok: There's too much government secrecy.

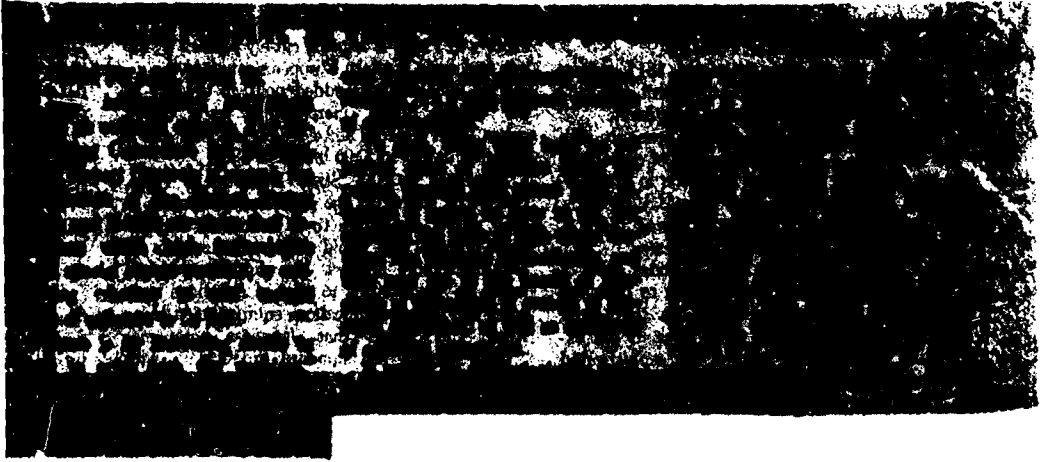
MARTIN ALLENBERG—TIME

U.S. May Turn to Electronic Warfare

The War Relocation Authority today announced that it has received a grant from the War Relocation Authority to fund a program of electronic warfare research. The program is being conducted by the War Relocation Authority in cooperation with the War Relocation Authority and the War Relocation Authority.

U.S. May Turn to Electronic Warfare
Electronic Warfare Control System
 Administration Plans to Develop
 of Program, Dept. of War

The War Relocation Authority today announced that it has received a grant from the War Relocation Authority to fund a program of electronic warfare research. The program is being conducted by the War Relocation Authority in cooperation with the War Relocation Authority and the War Relocation Authority.



N. Y. Times
Oct. 15, 1984

Reagan Orders Action on Eavesdropping

By DAVID BURNHAM

Special to The New York Times

WASHINGTON, Oct. 14 — President Reagan, acting on an intelligence report that Soviet eavesdropping is a serious security threat, has ordered the creation of a cabinet-level group to combat it.

Mr. Reagan signed a directive three weeks ago spelling out the extent of the threat and ordering a Government move to reduce the loss of Government and private industry information that might help the Soviet Union or other nations.

According to the unclassified version of the President's order, equipment that is used to eavesdrop on telephone conversations and other kinds of electronic messages is now widely available and "is being used extensively by foreign nations." The order added that the technology "can be employed by terrorist groups and criminal elements."

With the widespread use of microwave towers and satellites to transmit telephone messages and other data, the messages of Government, businesses and individuals have become increasingly subject to interception. Antennas in Cuba and on Soviet trawlers cruising offshore reportedly are able to identify and record much of this traffic.

Special Telephone Equipment

While the Ford and Carter administrations were concerned about the problem and ordered some changes in Government practices to deal with it, Mr. Reagan's National Security Decision Directive 145 is the first public assertion by a President that international eavesdropping constitutes a threat to the United States.

The President's directive was obtained after Walter G. Dealey, the National Security Agency's deputy director for communications security, disclosed in an interview that the agency hoped to equip Government and industry with 500,000 special telephones. The telephones are meant to make it far more difficult for eavesdroppers to conduct electronic surveillance.

Mr. Reagan said that both Government and privately owned communication networks currently transmit large amounts of classified and unclassified information that, when put together, can reveal important secrets.

"The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests," Mr. Reagan's directive said.

"A comprehensive and coordinated approach must be taken to protect the Government's telecommunications and automated information systems against current and anticipated threats," the document continued.

"This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities."

Cabinet-Level Steering Group

The directive, written by the staff of the National Security Council, established the Systems Security Steering Group, made up of the Secretaries of State, Treasury and Defense, the Attorney General, the director of the Office of Management and Budget and the Director of Central Intelligence.

In addition to setting overall policies, the directive said the steering group was responsible for reviewing all communication security proposals before they were submitted "to the Office of Management and Budget for the normal budget review process."

The directive's explicit requirement that the budget office review and approve all electronic security programs appeared to thwart efforts by the National Security Agency, which suggested this summer that it should become the "national focal point for communications security requirements and funding."

Agency Has Twin Missions

The National Security Agency is the nation's largest and most secret intelligence organization. With an estimated annual budget of \$4 billion, its twin missions are to collect electronic intelligence all over the world and protect the sensitive communications of the United States. It also serves as the principal adviser to the President and the National Security Council on communication security questions.

President Reagan's directive set up the National Telecommunications and Information Systems Security Committee, subordinate to the cabinet level steering group. This committee has 14 members, including the Chairman of the Joint Chiefs of Staff, the Director of the Federal Bureau of Investigation and the director of the top security agency. The committee was ordered to establish two subcommittees, one focusing on telephone security and the other on computer security.

In a third major assignment, Mr. Reagan authorized the security agency to serve as the "national manager" for telephone and computer security. In this role, the agency was authorized to conduct, approve or endorse all Government research on this problem.

The President's directive also orders the agency to examine Government

telecommunications and computer systems to determine their "vulnerability to hostile interception and exploitation."

The order explicitly authorized the Agency to monitor "official communications" but added that such monitoring "shall be conducted in strict compliance with the law, Executive Orders and applicable Presidential directives."

The Presidential directive did not say the agency had the right to monitor the communications of private corporations, but guidelines under which such monitoring may be conducted were approved by Attorney General William French Smith earlier this year in a letter to Lincoln D. Fausch, director of the security agency. The guidelines said:

"The Government shall not monitor telecommunications systems which are owned or leased by Government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization."

The Attorney General's rules added that monitoring by the security agency or other Government agencies should not be begun until steps "have been implemented sufficiently to afford adequate notice to the contractor organization's employees."

But the guidelines noted that "information acquired incidentally from government telecommunications during the course of authorized communication security monitoring which related directly to a significant crime" should be referred to the military commander or law enforcement agency with jurisdiction.

"The results of monitoring may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency which performed the monitoring," the guidelines said.

Law

The No Man's Land of High Tech

New devices aid police but threaten the right of privacy

On the morning of Nov. 2, 1983, Francis Lynch, then chief of detectives of the Woonsocket, R.I., police department, got a strange call. "You may think I'm crazy," said an excited young woman, "but there is some guy dealing drugs, and I can hear it on my radio." Lynch was skeptical, but he sent two detectives to the woman's house.

It turned out that the transmissions that the woman had heard on her AM radio were coming from a nearby home whose occupant, Leo DeLaurier, owned a cordless telephone. DeLaurier was apparently unaware that such devices are little more than short-range radio transmitters whose signals can sometimes be picked up by ordinary radio receivers. During the next month, the police say, they recorded more than 100 hours of incriminating conversations by DeLaurier about the sale of cocaine and marijuana. Then they arrested DeLaurier, his wife and 22 other people on drug charges. DeLaurier objected to the use of the tapes, and his trial has been postponed pending the outcome of an appeal to the Rhode Island Supreme Court. DeLaurier argues that the monitoring of his phone was an illegal invasion of his privacy since it was done by the police without a warrant.

Legal experts point out that cordless phones are one of many new-age technological devices that fall into a legal no man's land, an ambiguous region inhabited by such consumer products as personal computers and the ubiquitous message beepers and by sophisticated police equipment like mini-video cameras. The lack of clear legal rules for police use of the equipment promises to keep the courts busy. Just last month two federal courts clashed on the issue when the U.S. Court of Appeals for the Seventh Circuit in Chicago overruled a federal district court and found that video surveillance of four suspected members of the Puerto Rican terrorist group FALN did not violate the Fourth Amendment's guarantee against "unreasonable searches and seizures." Says University of Chicago Law Professor Geoffrey Stone: "Technology—bugs, beepers that police attach to cars, parabolic microphones—all of this enables the Government to invade privacy in ways far more extreme than one could possibly have imagined when the Fourth Amendment was written."

The Kansas Supreme Court was the first state high court to rule on the cordless-phone issue, holding last March that those who use such phones are broadcast-

ing over the public air waves and have "no reasonable expectation of privacy," a finding that may surprise the 7 million or so owners of the popular instruments. But to rule otherwise, Rhode Island's attorneys argued before that state's supreme court, could mean that the woman who inadvertently overheard DeLaurier's conversations might be held criminally liable for violating the federal wiretapping law.



DeLaurier's lawyer, however, asserted that this 1968 legislation, which forbids wiretapping without court authorization, does apply to cordless phones, since the statute defines a "wire communication" as any conversation that is carried "in whole or in part" by wire. Even cordless instruments must utilize regular phone lines at some point to transmit calls.

Video surveillance is as knotty an issue as the new telephones. Abcam, the De Lorean drug investigation and other well-publicized "sting" operations have made it seem that police have broad authority to videotape criminal activity. In fact, cameras have usually been employed to record only those meetings where an undercover agent or informer with prior knowledge of the filming is also in the room. This was not the situation in the Chicago FALN case, in which the FBI had authorization for both audio and video surveillance from a federal judge. The agency resorted to the video surveillance of two "safe house" apartments after two of the four suspects successfully thwarted wiretaps and bugs.

Once the cameras had been installed, agents say, they observed some of the defendants constructing time bombs. The four were arrested in June 1983 on seditious-conspiracy and weapons charges when the FBI learned that they allegedly planned to mark the July 4 holiday by blowing up military installations.

U.S. District Judge George Leighton threw out the FBI's 130 hours of videotape evidence in 1984, saying that "no one, not even in the name of ferreting out crime, has the right to invade the privacy of a home" without proper legal authority. He ruled that the 1968 wiretap law provided no such authority because it says nothing about video surveillance. The Seventh Circuit panel, in an opinion written by Supreme Court hopeful Richard Posner, held that the wiretap law did not apply but found that video surveillance is permitted under the Constitution without specific legislative approval. Paraphrasing a famous dissent by Justice Louis Brandeis, Posner wrote, "There is no right to be let alone while assembling bombs in safe houses." The accused FALN members plan to appeal the ruling to the U.S. Supreme Court.

Many legal observers are frightened by the prospect of widespread video surveillance. Raising the specter of *Nineteen Eighty-Four* and Big Brother, Herman Schwartz, a law professor at American University, denounces it as "very dangerous" to everyone's civil liberties. Harvard Law Professor Laurence Tribe cautions that technological innovations like video cameras may be rendering the traditional protections of the Fourth Amendment "irrelevant." Columbia University Law Professor Richard Uviller, a former prosecu-

tor, says of the new high-tech snooping, "When there is no alternative, when the crime is terror, there is a strong law-enforcement need for this." But he adds that "its uses should be reserved for only the most serious circumstances: kidnaping, murder, espionage and terrorism."

To clarify the legal muddle, several federal statutes have been proposed, including one by Wisconsin Congressman Robert Kastenmeier that would force police to satisfy a series of strict requirements in order to get a warrant for video prying. Though the Kastenmeier bill died in the last Congress, it will be reintroduced in this session. Judges, legislators and civil libertarians agree that the privacy problems presented by technological changes make necessary a new assessment of existing statutes and court rules. Warns John Shattuck, a former American Civil Liberties Union official, "In many ways, technology is now outstripping the law." —By Michael S. Baum

Reported by Carol Fletcher/Chicago and Timothy Loughran/New York



U.S. Department of Justice

Criminal Division

Office of the Assistant Attorney General

Washington, D.C. 20530

27 DEC 1983

Honorable Robert W. Kastenmeier
 Chairman
 Subcommittee on Courts, Civil
 Liberties and the Administration
 of Justice
 Committee on the Judiciary
 House of Representatives
 Washington, D.C. 20515

Dear Mr. Chairman:

The Attorney General has asked me to respond to your letter of December 1, 1983, regarding wiretapping.

Our records for Title III wiretaps commence with January 1969; thus, we have no figures for 1968. The following items represent statistics for the period of January 1969 to September 1983 that are responsive to your individual requests:

- (1) Total number of wiretap applications approved - 2,710
- (2) (a) Initial applications - 2,018
 Extensions - 692
- (b) Requests by Department of Justice agencies

FBI	-	2,128
DEA	-	325
DEA predecessors	-	0
ODALE	-	0
BNDD	-	135
INS	-	0
- (c) Types of violations

Gambling	-	1,048
Narcotics	-	708
Loansharking	-	150
Counterfeiting	-	24
Kidnapping	-	13
Obstruction of Justice	-	19
Bribery	-	26

Theft	-	20
Racketeer Influenced and Corrupt Organization	-	465
Interstate Transportation of Stolen Property	-	84
D.C. Code	-	34
Explosives	-	36
Extortion	-	34
Murder	-	4
Bank Robbery	-	13
Riot	-	2
Bankruptcy	-	3
Soliciting Pension Fund	-	11
Espionage	-	3
Public Corruption	-	13

It should be noted that frequently more than one offense is cited in a wiretap application. For reporting purposes we maintain statistics only on the lead or main offense in each request. The list in item (2)(c) above reflects that practice.

~~If you should require further assistance, please contact us.~~

Sincerely,

Stephen S. Trott
Assistant Attorney General
Criminal Division

By:

James Knapp
Deputy Assistant Attorney General
Criminal Division

	1982	1983	1984	1985
Requests for permission to close all or part of a judicial proceeding processed	8	14	20	25
New Witness Security Program Requests	348	344	360	360
Matters Concerning				
Witnesses from Prior Years	30	30	30	30
Prisoner-Witness Matters	235	240	260	260
Title III Requests	248	383	475	525
Confidential Fund Requests	0	0	1	1
Requests for Use of Hypnosis	48	44	45	45
Requests for Use of FBI Equipment	1	1	3	3
Statistical Reports				
(Title III/Consensual)	69	69	69	69
Statistical Reports				
(Witness Security Program)	71	71	71	71
Witnesses Accepted into Program	300	294	325	325
Emergency MSP Requests Authorized	6	9	10	10
Wiretaps Approved	226	359	450	500
<u>Asset Forfeiture Office</u>				
<u>Major Cases in which the Office Has Substantial Involvement</u>				
Pending, beginning of year	...	5	2	7
Opened	...	1	10	78
Closed	...	4	5	25
Pending, end of year	...	2	7	60
<u>Major Ongoing Startup and Support Projects</u>				
Responses to Inquiries from the Field	...	578	2,000	2,500
Resolution and Mitigation Petitions Reviewed	...	135 2/	480	500

19 87
 Criminal
 Div

D.O.S

915 Budget Sub Minister

TITLE III's

Department of Justice Agencies

<u>Calendar Year</u>	<u>Originals</u>	<u>Extensions</u>	<u>Total</u>	<u>FBI</u>	<u>DEA</u>	<u>ODALE</u>	<u>BNDD</u>
1969	33	12	45	34			4
1970	192	39	231	177			51
1971	295	58	353	316			25
1972	208	47	255	184			32
1973	159	41	200	143	16		23
1974	118	21	139	115	23		
1975	107	11	118	94	19		
1976	147	18	165	135	28		
1977	81	17	98	68	24		
1978	86	29	115	92	23		
1979	102	57	159	138	16		
1980	87	39	126	88	29		
1981	103	61	164	121	34		
1982	148	110	258	206	50		
1983 -9/83	<u>152</u>	<u>132</u>	<u>284</u>	<u>217</u>	<u>63</u>		
Totals	2018	692	2710	2128	325	8	135

TITLE III's

	FY 1983	FY 1982	FY 1981	FY 1980	FY 1979	FY 1978	FY 1977	7/76-9/76	FY 1976	FY 1975	FY 1974	FY 1973	FY 1972	FY 1971	FY 1970	FY 1969	TOTAL
Gambling	5	2	19	4	8	21	41	9	70	82	72	146	243	243	80	3	1048
Marcotics	193	115	44	34	21	25	24	8	32	12	30	56	37	49	25	3	708
Loansharking	11	8	14	16	4	11	10	1	11	9	15	11	5	10	13	1	150
Counterfeiting	3	0	0	0	2	0	4	0	1	1	0	3	6	1	0	3	24
Kidnapping	6	0	0	2	0	3	1	0	0	0	0	0	0	0	1	0	13
Obstruct Justice	0	0	7	1	4	0	2	0	2	1	0	0	0	1	0	1	19
Bribery	6	2	7	0	0	4	0	0	0	0	1	1	5	0	0	0	26
Theft	5	4	2	0	4	0	0	0	1	0	0	2	2	0	0	0	20
RICO	108	67	53	42	91	35	16	10	23	11	3	2	4	0	0	0	465
ITSP	5	5	5	7	4	9	11	3	8	6	11	6	1	0	3	0	84
D. C. Code	0	0	0	3	3	1	1	0	2	3	2	14	4	1	0	0	34
Explosives	16	5	7	0	0	0	1	0	6	0	0	0	1	0	0	0	36
Extortion	0	0	8	4	4	0	3	0	2	0	2	10	1	0	0	0	34
Murder	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	4
Bank Robbery	0	7	0	1	0	0	1	0	1	0	1	0	0	0	2	0	13
Riot	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	2
Bankruptcy	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	3
Soliciting Pension Fund	0	0	0	4	4	0	1	0	0	0	0	2	0	0	0	0	11
Espionage	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	3
Public Corruption	0	10	3	0	0	0	0	0	0	0	0	0	0	0	0	0	13
Totals	355	226	169	118	150	109	124	31	160	125	137	253	309	305	124	11	2710