"(A) all available forms of such assistance,

"(B) any specific criteria which must be met to qualify for each type of assistance that is available, and

"(C) any limitations which apply to each type of assistance.

"(3) Offers of assistance under this section shall—account for—

"(A) the location of and travel time to—

"(i) the applicant's place of business; and

"(ii) schools which the applicant or members of the applicant's family who reside with the applicant attend;

"(B) the applicant's need for access to—

"(i) the site of a home or place of business whose destruction or damage is the result of the major disaster which created the applicant's need for assistance under this section: and

"(ii) crops or livestock which the applicant tends in the course of any involvement in farming which provides 25 percent or more of the applicant's annual income; and

"(C) the applicant's desire to remain in the same community.

"(4) An offer of assistance under this section shall remain available for acceptance for 60 days after the date on which such offer is made.

"(5)(A) If an applicant's eligibility for assistance is withdrawn after two offers of assistance have been made to such applicant, or if an offer of assistance is withdrawn after the 60 day period referred to in paragraph (4)—

"(i) the applicant shall, upon request, be granted a hearing to show cause why such eligibility for assistance of offer of assistance should not be withdrawn;

"(ii) the procedures for such hearing shall be the same as those which apply in a hearing to dispute a proposed termination of or eviction from temporary housing assistance and shall be fully explained to the applicant; and

"(iii) the applicant shall be given assistance in preparing for and presenting arguments at such hearing.

"(B) A final determination on any withdrawal of eligibility or an offer of assistance shall be made within ten working days after the date on which a hearing is requested under this paragraph."

SEC. 5. INCREASE IN AMOUNTS OF INDIVIDUAL AND FAMILY GRANTS.

Section 408(b) of section 601 of the Disaster Relief Act of 1974 (Public Law 93-188; 42 U.S.C. 5121 et seq.) is amended by striking "$5,000" and inserting "$7,500".

PROCESS IN CERTAIN GRANTS OF ASSISTANCE

Subsection (a) of section 601 of the Disaster Relief Act of 1974 is amended—

(1) by inserting "(1)" after "(a)", and

(2) by adding at the end the following new paragraph:

"(2) Rules and regulations authorized by paragraph (1) shall provide that payment of any assistance under this Act to a State or local government or to an eligible non-profit organization shall be completed within 60 days after the date on which an applicant submits a claim after completion of the approved work.●

● Mr. FORD. Mr. President, I wish I could say that I am pleased to join my friend from Pennsylvania in sponsoring these two bills, but I cannot. The reason for my displeasure is that there should be no need for such legislation. If there were only one role for the Federal Government after providing for the national defense, it should be disaster assistance to the States. But the Federal Emergency Management Agency—created to come to the rescue of the States in time of catastrophe—wants to cut back drastically on the assistance it provides. That is shameful.

So, you see why I take no pleasure in sponsoring this legislation. It is introduced only to prevent FEMA from making a serious mistake. The Agency's proposed rule would be devastating to Kentucky, Pennsylvania, Illinois, Indiana, Ohio, Michigan, and Wisconsin. However, I also suspect it would be just as harmful to States of the Midwest and the Great Plains, which regularly are hit by tornados—to California, which is hit by mudslides and brushfires every year—to the Gulf and Atlantic Coast States regularly lying in the path of hurricanes.

In fact, Mr. President, if the legislation we are introducing today is not signed into law before FEMA's proposed rule becomes final, every State in the Union will run the risk of being unable to respond adequately if hit by a natural disaster. I commend the Senator from Pennsylvania [Mr. HEINZ], for recognizing the potential danger of FEMA's rule, and for taking action to prevent it; and I hope my colleagues will join us in this effort.●

● Mr. LAUTENBERG. Mr. President, I am pleased to join today with my colleague from Pennsylvania, Senator Heinz, in introducing legislation to retain current Federal Emergency Management Agency policy on disaster relief.

In May, the Federal Emergency Management Agency issued draft regulations on disaster relief which, unless Congress intervenes, will become effective in October. The purpose of these regulations is to save FEMA money. The impact of the regulations is to make many communities suffering natural disasters ineligible for Federal assistance.

Mr. President, of the last 111 Presidential declarations of disasters, only 61 would be eligible for assistance under the new FEMA rules. Those found eligible for assistance would find themselves called upon to cover a far higher percentage of the cleanup and rehabilitation costs. FEMA would establish a scale of ability to pay based on per capita income. The fairness of such a sliding scale is worthy of debate and should, if it is to be implemented at all, be done legislatively and not by regulation.

To provide an example of the impact of these new regulations in New Jersey, I asked my State Office of Emergency Management to compare the cost to communities devastated by the 1984 spring floods. Passaic County, NJ had $1,664,000 in damages. After the Presidential declaration of disaster, the Federal Government paid $1,247,000 with the local match being $416,000. Under the new regulations, the local share would be $1,013,000, with FEMA covering $650,000.

Mr. President, historically, natural disasters have not been considered to be the fault of local communities and the Federal Government has attempted to quickly provide emergency relief. Until recently, the Federal Government covered 100 percent of disaster relief costs. In order to control costs, FEMA, without legislative mandate, began the 75/25 percent match with localities. That practice has not proven to be burdensome in most circumstances. Now it appears that FEMA wants to shift the burden of disaster relief primarily to States and localities.

Mr. President, the bill we are introducing will, for the first time, put in statute the 75/25 percent matching requirement. The bill will prevent FEMA from imposing, by regulation, the per capita scale which would rule States and localities ineligible for relief. The bill will prevent FEMA from adopting a 50/50 percent match.

Mr. President, as ranking minority member of the Environment and Public Works Committee's Subcommittee on Regional and Community Development, I will push for hearings on this issue. Disaster relief is one of the basic functions of Government. I strongly favor efforts to reduce unnecessary Federal spending, but I do not support efforts to save money at the expense of communities devastated by floods, hurricanes, coastal storms and other natural disasters.

I am pleased to be an original cosponsor of this legislation and urge its swift consideration and adoption.●

By Mr. LEAHY (for himself and Mr. MATHIAS):

S. 2575. A bill to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes; to the Committee on the Judiciary.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Mr. LEAHY. Mr. President, today I am introducing the Electronic Communications Privacy Act with Senator MATHIAS. The need for this legislation to update our legal privacy protections and bring them in line with modern telecommunications and computer technology is clear if we consider some simple illustrations.

In the first example, two business people are discussing their company's sensitive financial data over the telephone. Unknown to them, a competitor is using a phone tap to listen in on their conversation. Across town, a police officer has a hunch that Jane Doe is involved in drug trafficking. He goes to the Post Office and tells the postal clerk that he wants to intercept, open and read Ms. Doe's mail, and then have it resealed and delivered.

We would all agree that the competitor eavesdropper's conduct is wrong and the policeman's conduct is wrong. Their conduct is also illegal.

Now let me change the scene just a little and remind my colleagues that each example is probably going on

somewhere in the United States right now.

Instead of the two business people discussing financial matters over the telephone, they use a video teleconference system which displays their data on their video screens. The same data is picked up by their competitor. Instead of going to the Post Office, the police officer goes to an electronic mail company. Ms. Doe is a user of the system and the officer asks to see all of Ms. Doe's messages.

The only real difference between the eavesdropper's and the policeman's conduct is that in the second example, traditional telephone or mail communications have been replaced by one of the great technological innovations available in America today. Many of our constituents who use those new forms of technology in their homes and in their businesses would be surprised to learn that the same conduct is not clearly illegal once the electronic component is added to the story.

The Electronic Communications Privacy Act is designed to update our law to provide a reasonable level of Federal privacy protection to these new forms of communications. It is the culmination of 2 years of hard work. I want to commend the Senator from Maryland, the chairman of the Senate Judiciary Committee's Subcommittee on Patents, Copyrights and Trademarks for his support and his efforts in developing this legislation.

I also want to congratulate Congressman BOB KASTENMEIER and Congressman CARLOS MOORHEAD, the chairman and ranking minority member of the House Judiciary Committee's Subcommittee on Courts, Civil Liberties and the Administration of Justice. The Congressmen and their staffs saw the House Judiciary Committee unanimously pass this landmark legislation last week.

Mr. President, let me just briefly describe the limitations of current law and the development of this legislation. The Federal wiretap statute, title III of the Omnibus Crime and Safe Streets Act of 1968 is our primary law protecting the security and privacy of business and personal communications.

Eighteen years ago, when title III was written, Congress could not appreciate—or in some cases even contemplate—telecommunications and computer technology we are starting to take for granted today: electronic mail, computer-to-computer data transmissions, cellular telephones, paging devices, and video teleconferencing. Lawmakers in 1968 could not imagine the extensive use of computers for the storage and processing of information which has put a wide range of personal and business records, including health, financial, and other records, "on-line," or the ready availability of electronic hardware, including high-technology video and radio surveillance systems, making it possible for overzealous law enforcement agencies, industrial spies, and just plain snoops to intercept the personal or proprietary communications of others.

Nor could Congress envision the dramatic changes in the telephone industry which we have witnessed in the last few years. Today, a phone call can be carried by wire, microwave, or fiber optics. Even a local call may follow an interstate path. And an ordinary phone call can be transmitted in different forms—digitized voice, data or video. In addition, since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services.

When Congress enacted title III, it had in mind one kind of communication—voice—and one kind of transmission—a transmission via a common carrier analog—or regular voice—telephone network. Congress chose to cover only the "aural acquisition" of the contents of a common carrier wire communication. The Supreme Court has interpreted that language to mean that to be covered by title III, a communication must be capable of being overheard.

Title III of the Omnibus Crime and Safe Streets Act is hopelessly out of date. It applies only to interceptions of voice communications transmitted via common carrier. It does not cover data communications. It does not specify whether or how communications made using electronic pagers or the private transmissions of video signals like those used in teleconferencing are protected.

Our 2-year effort to deal with this gap between the law and technological innovation began in 1984 when I asked the Attorney General whether he believed interceptions of electronic mail and computer-to-computer communications were covered by the Federal wiretap laws.

The Criminal Division of the Department of Justice replied that Federal law protects electronic communications against unauthorized acquisition only where a reasonable expectation of privacy exists. Underscoring the need for this legislation, the Department concluded: "In this rapidly developing area of communications which range from cellular nonwire telephone connections to microwave-fed computer terminals, distinctions, such as—whether there does or does not exist a reasonable expectation of privacy—are not always clear or obvious."

Hearings in the 98th Congress held by Senator MATHIAS and myself in the Senate Judiciary Committee and by Congressman KASTENMEIER in the House Judiciary Committee demonstrated the scope of these problems and the need to act. We began working with the Justice Department and many individuals, businesses, industry groups, and civil liberty groups. Those groups were concerned primarily about the need to update the law to better protect communications privacy. They also pointed out that the absence of such privacy protections may be inhibiting further technological development in this country and that enactment of such privacy protections will encourage the full use of modern computer technology available in America today.

During those discussions, two things became very clear. First, the need to address unauthorized acquisitions of information is very real. Communications companies have been faced with Government demands, unaccompanied by a warrant, for access to the messages contained in electronic mail systems. And the unwanted private intruder, whether a competitor or a malicious teenager, can do a great deal of damage before being discovered—if he or she is ever discovered. Second, encryption is not the answer. It can be broken. More importantly, the law must protect private communications from interception by others.

The product of our discussions with the Department of Justice and private groups interested in promoting communications privacy, while protecting legitimate law enforcement needs and promoting technological innovation, was S. 1667, which Senator MATHIAS and I introduced last September. Congressmen KASTENMEIER and MOORHEAD introduced identical legislation in the House.

Shortly thereafter, the Office of Technology Assessment issued its report, "Electronic Surveillance and Civil Liberties." Again, the need for this legislation was underlined. OTA concluded that a message sent by means of an electronic mail system could be intercepted and that its contents could be disclosed to an unintended snoop. The Office of Technology Assessment study also concluded that current legal protections for electronic mail are "weak, ambiguous, or nonexistent," and that "electronic mail remains legally as well as technically vulnerable to unauthorzed surveillance."

Since that time, the Subcommittee on Patents, Copyrights, and Trademarks and the House Judiciary Committee's Subcommittee on Courts, Civil Liberties, and the Administration of Justice have held extensive hearings on the legislation. During those hearings, the Department of Justice and radio hobbyists raised some concerns about the bill. Those concerns are addressed in this new version of the Electronic Communications Privacy Act we are introducing today. This is the same language that the House Judiciary Committee passed by a vote of 34 to 0 last week.

The bill will extend coverage of title III of the Omnibus Crime and Safe Streets Act beyond only voice communications to include video and data communications. It recognizes that private carriers and common carriers

perform so many of the same functions today that a distinction between privacy standards is not warranted. The bill also creates penalties for the unauthorized access of electronically stored information if that information is obtained or altered.

In order to address radio hobbyists' concerns, we modified the original language of S. 1667 to clarify that intercepting traditional radio services is not unlawful. Under this revised Electronic Communications Privacy bill, cellular phones, private and public microwave services and voice or display pagers are protected against interception. Cordless telephones and tone-only pagers are not.

The Electronic Communications Privacy Act provides standards by which law enforcement agencies may obtain access to both electronic communications and the records of an electronic communications system. These provisions are designed to protect legitimate law enforcement needs while minimizing intrusions on the privacy of system users as well as the business needs of electronic communications system providers.

At the request of the Justice Department, we strengthened the current wiretap law from a law enforcement perspective. Specifically, we expanded the list of felonies for which a voice wiretap order may be issued and the list of Justice Department officials who may apply for a court order to place a wiretap. We also added a provision making it easier for law enforcement officials to deal with a target who repeatedly changes telephones to thwart interception of his communications, and created criminal penalties for those who notify a target of a wiretap in order to obstruct it.

The bill creates a statutory framework for the authorization and issuance of an order for a pen register. It also creates civil penalties for the users of electronic communications services whose rights under the bill are violated. Finally, it preserves the careful balance governing electronic surveillance for foreign intelligence and counterintelligence purposes embodied in the Foreign Intelligence Surveillance Act of 1978. And it provides a clear procedure for access to telephone toll records in counterintelligence investigations.

Mr. President, the subcommittee staff has prepared a more detailed summary of the bill. I ask unanimous consent that the summary, along with the text of the bill, be printed in the RECORD following my remarks.

From the beginning of our history, first-class mail has had the reputation of preserving privacy while promoting commerce. It is high time we updated our laws so that we can say the same about new forms of technology which are being use side by side with first-class mail. A broad coalition of businesses, industry groups, civil liberties groups, and privacy groups are asking us to do that by enacting the Electronic Communications Privacy Act. The Department of Justice also strongly supports this legislation, and I look forward to working with my colleagues to see it passed and signed into law this year.

In closing, let me just thank the staff who have worked so hard, not only in drafting a good bill, but in working together until they successfully addressed the concerns raised during the hearings. The bill now enjoys the broadest possible support and is ready for prompt passage in the House and Senate, thanks to their efforts.

There being no objection, the previously mentioned material was ordered to be printed in the RECORD, as follows:

S. 2575

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception";

(C) by striking out "as a common carrier"; and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

(B) by inserting ", electronic," after "wire".

(4) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(5) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequence allocated under part 74 that is not exclusively allocated to broadcast auxiliary service, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTION WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(2) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(3) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title);

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

"(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "and electronic communications" after "wire".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication sevice" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided*, That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2512(2)(a) of title 18, United States Code is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended by striking out "communication common carrier" and inserting "provider of electronic communication service" in lieu thereof.

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.".

(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) *or 2517 of this title*;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) IN GENERAL.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) COMPUTATION OF DAMAGES.—The court may assess as damages in an action under this section whichever is the greater of—

"(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney

General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relation to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),"; and

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) the location of any fugitive from justice from an offense described in this section; or"; and

(4) by redesignating paragraph (h) as paragraph (j).

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF 30-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonable available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.".

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end of the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(i) in the case of an application with respect to the interception of an oral communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(III) the judge finds that such specification is not practical; and

"(ii) in the case of an application with respect to a wire or electronic communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(III) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

SEC. 107. INTELLIGENCE ACTIVITIES.

(A) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechancial device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice of attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence

Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.".

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception.".

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

(2) the date two years after the date of the enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

"Sec.
"2701. Unlawful access to stored communications
"2702. Disclosure of contents.
"2703. Requirements for governmental access
"2704. Backup preservation.
"2705. Delayed notice.
"2706. Cost reimbursement.
"2707. Civil action.
"2708. Exclusivity of remedies.
"2709. Counterintelligence access to telephone toll and transactional records.
"2710. Definitions.

"§ 2701. Unlawful access to stored communications

"(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703 or 2704 of this title.

"§ 2702. Disclosure of contents

"(a) PROHIBITIONS.—Except as provided in subsection (b)—

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communications to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

"(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

"(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant;

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

"(2) Paragraph (1) is applicable with respect to any electronic communications that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriberr or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATIONS SERVICE OR REMOTE COMPUTING SERVICE.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

"(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(3) obtains a court order for such disclosure under subsection (d) of this section.

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

"§ 2704. Backup preservation

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) CUSTOMER CHALLENGES.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

"§ 2705. Delayed notice

"(a) DELAY OF NOTIFICATION.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days; if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3) destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"§ 2706. Cost reimbursement

"(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall in-

clude any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) CAUSE OF ACTION.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discoverd or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records

"(a) DUTY TO PROVIDE.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) PROHIBITION OF CERTAIN DISCLOSURE.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.".

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access . . . . . 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

SEC. 301. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS

"Sec.

"3121. General prohibition on pen register use; exception.

"3122. Application for an order for a pen register.

"3123. Issuance of an order for a pen register.

"3124. Assistance in installation and use of a pen register.

"3125. Reports concerning pen registers.

"3126. Definitions for chapter.

"§ 3121. General prohibition on pen register use; exception

"(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveilliance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent or the user of that service.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for a order for a pen register

"(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmantion, to a court of competent jurisdiction of such State.

"(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER.—An order authorizing or approving the installation and use of a pen register shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless otherwise ordered by the court.

"§ 3124. Assistance in installation and use of pen register

"(a) IN GENERAL.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) COMPENSATION.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"§ 3125. Reports concerning pen registers

"The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'wire communication' has the meaning set forth for such term in section 2510 of this title;

"(3) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

"(4) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers ..... 3121".

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

A SUMMARY OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968—the federal wiretap law—to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law to update and clarify federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies. Originally introduced in the Senate as S. 1667 by Senators Leahy and Mathias, and H.R. 3378 by Congressman Kastenmeier and Moorhead, the bill has gone through a substantial revision as a result of negotiations with affected industry groups and the Department of Justice. On June 11, the House Judiciary Committee unanimously reported the product of these negotiations which has been reintroduced as H.R. 4952. The Justice Department strongly supports this legislation. Highlights of the bill follow:

Currently, Title III covers only voice communications. The bill expands coverage to include video and data communications.

Currently, Title III covers only common carrier communications. The bill eliminates that restriction since private carriers and common carriers perform so many of the same functions today that the distinction no longer serves to justify a different privacy standard.

At the request of the Justice Department, the bill continues to distinguish between electronic communications (data and video) and wire or oral communications (voice) for purposes of some of the procedural restrictions currently contained in Title III. For example, court authorization for the interception of a wire or oral communication may only be issued to investigate certain crimes specified in Title III. An interception of an electronic communication pursuant to court order may be utilized during the investigation of any federal felony.

Certain electronic communications are exempted from the coverage of the bill including the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit; tone only paging devices; amateur radio operators and general mobile radio services; marine and aeronautical communications systems; police, fire, civil defense and other public safety radio communications systems; the satellite transmission of network feeds; the satellite transmission of satellite cable programming as defined in Section 705 of the Communications Act of 1934; any other radio communication which is made through an electronic communications system that is configured so that such communication is "readily accessible to the general public," a defined term in the bill.

The term readily accessible to the general public does not include communications made by cellular radio telephone systems; therefore, the bill continues current restrictions contained in Title III against the interception of telephone calls made on cellular telephone systems. However, the criminal penalty for an unlawful interception of a cellular phone call is reduced from the current five-year felony to a six-month petty offense.

The bill expends the list of felonies for which a voice wiretap order may be issued. It also expands the list of Justice Department officials who may apply for a court order to place a wiretap.

The bill creates a limited exception to the requirement that a wiretap order designate a specific telephone to be intercepted where the Justice Department makes a showing that the target of the wiretap is changing telephones to thwart interception of his or her communications.

The bill makes it a crime for a person who has knowledge of a court authorized wiretap to notify any person of the possible interception in order to obstruct, impede or prevent such interception.

Title II of the bill creates parallel privacy protection for the unauthorized access to the computers of an electronic communications system, if information is obtained or altered. It does little good to prohibit the unauthorized interception of information while it is being transmitted, if similar protection is not afforded to the information while it is being stored for later forwarding.

The bill establishes criminal penalties for any person who willfully accesses without authorization a computer through which an electronic communication service is provided and obtains, alters or prevents authorized access to a stored electronic communication. The offense is punished as a felony if committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain; otherwise it is punished as a petty offense.

Providers of electronic communication services to the public and providers of remote computing services to the public are prohibited from willfully divulging the contents of communications contained in their systems except under circumstances specified in the bill.

The contents of messages contained in electronic storage of electronic communications systems which have been in storage for 180 days or less may be obtained by a government entity from the provider of the system only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant.

The content of messages stored more than 180 days and the contents of certain records stored by providers of remote computer processing services may be obtained from the provider of the service without notice to the subscriber if the government obtains a warrant under the Federal Rules of Criminal Procedure or with notice to the customer pursuant to an administrative subpoena, a grand jury subpoena, or a court order based on a showing that there is reason to believe that the contents of the communication are relevant to a legitimate law enforcement inquiry. Provisions for delay in notice are also included.

Civil penalties are created for users of electronic communications services whose rights under the bill are violated.

The bill creates a statutory framework for the authorization and issuance of an order for a pen register based on a finding that such installation and use is relevant to an on going criminal investigation.

Mr. MATHIAS. Mr. President, today I am pleased to join with the junior Senator from Vermont, [Mr. LEAHY], to introduce the Electronic Communications Privacy Act of 1986. This legislation is an essential element in our efforts to strengthen the protection of Americans' right to privacy in an era of ever more pervasive electronic communications media.

The bill we introduce today is a revised version of S. 1667, which Senator LEAHY and I introduced on September 19, 1985. It is also identical to H.R. 4952, as unanimously approved earlier this month by the Judiciary Committee of the House of Representatives.

This bill has the same goal as S. 1667: To protect the privacy of Americans against unwanted and unwarranted intrusions. It adopts the same means to that goal: An updating of the 1968 Federal wiretap statute to bring fully within its ambit new communications technologies—including electronic mail, cellular telephone, and data transmissions between computers—that have transformed the ways in which Americans share information with each other and with the world. But our earlier bill has been improved by the process of hearings in both the Senate and the House, and extensive negotiations among interested parties in Government, private industry, and civil libertarians. The result is a bill that should enhance privacy protection, promote the development and proliferation of new communications technologies, and respond to the legitimate needs of law enforcement.

Technological advances are fast obliterating the distinctions among voice, video, and data transmission. Deregulation has made less meaningful the distinction between common carrier and private communications systems. And new means of sending and storing information are blurring the line between data in transmission and information in temporary electronic storage. This legislation responds to these developments by protecting the privacy of information in any electronic form, while it is in transmission or temporary storage, and without regard to the medium of its transmission. While the bill retains a few distinctions between the treatment of conventional telephone conversations and transmissions by other media, these differences appear reasonable and do not seriously detract from the principle of adapting the law to the technology of the present and future, rather than the past.

The Electronic Communications Privacy Act of 1986 specifies the circumstances under which law enforcement agencies may seek to intercept electronic communications or intrude into incidental electronic communications storage facilities. It also outlaws those intrusions unless undertaken pursuant to a warrant, and prohibits computer hacking directed against electronic communications systems if the result is to obtain, alter, or prevent access to a communication stored in the computer. The bill provides standards for third-party access to other data held by the operators of electronic communications services, and gives the customer of the service a civil remedy if these standards are not followed. Finally, this bill makes necessary improvements in the existing wiretap law to enhance the availability, usefulness and accountability of this key law enforcement tool. A more detailed discussion of the provisions of the Electronic Communications Privacy Act may be found in the summary that Senator LEAHY and I have inserted today in the CONGRESSIONAL RECORD.

Mr. President, the principles underlying this bill have long been supported by privacy advocates and by the affected communications industries, which know that business growth and continued innovation depend upon customer confidence that unauthorized snooping will be deterred and punished. That support continues, and has been strengthened by the improvements made in the bill in the legislative process in the other body. The administration in general, and the Attorney General in particular, have also been on record for a long time in support of the need to bring the wiretap laws up to date with modern technology. Attorney General Meese, when he appeared before the Judiciary Committee on January 29, 1985, seeking confirmation for the post he now holds, told the committee that one of his highest priorities as the chief law enforcement officer of the land would be "the safeguarding of individual privacy from improper governmental intrusion." During the same proceeding, he specifically noted electronic surveillance law as an area where new technology demanded updating. Given the Attorney General's strong views on privacy protection, I am particularly pleased to report to the Senate that the bill we introduce today has the vigorous and active support of the Department of Justice, not just as a general concept, but as a fully articulated legisalative package. While negotiations with the Jusice Department about this bill have been lengthy, they have resulted in a bill that the Department embraces as a vehicle for carrrying out the Attorney General's commitment to protect the privacy of Americans.

Mr. President, the bill we introduce today adds to S. 1667 the useful improvements crafted by our colleagues in the House of Representatives, particularly Representative ROBERT KASTENMEIER, chairman of the House Judiciary Subcommittee on Courts, Civil Liberties and the Administration of Justice, and Representative CARLOS MOORHEAD, that subcommittee's ranking minority member. I urge Senators to examine this legislation, to suggest any further refinements that may be necessary, and to join with me and with Senator LEAHY to see that it is speedily enacted into law.

By Mr. DURENBERGER (for himself, Mr. BAUCUS, Mr. DOLE, Mr. CHAFEE, Mr. HEINZ, Mr. CHILES, Mr. ANDREWS, Mr. ABDNOR, and Mr. MITCHELL):

S. 2576. A bill to amend title XVIII of the Social Security Act to require timely payment of properly submitted Medicare claims; to the Committee on Finance.

MEDICARE TIMELY PAYMENT AMENDMENTS

Mr. DURENBERGER. Mr. President, I rise today to introduce the "Medicare Timely Payment Amendments of 1986." This bill amends title XVIII of the Social Security Act to require Medicare to pay hospitals, doctors, and other health care providers promptly for services rendered to program beneficiaries as well as reimburse beneficiaries quickly when they file claims personally. My colleagues Senators BAUCUS, DOLE, BENTSEN, CHAFEE, HEINZ, CHILES, ANDREWS, ABDNOR, and MITCHELL are joining me in sponsoring this measure. S. 2576 is a companion to a bill of the same title being introduced today in the House of Representatives by Congressmen GRADISON and STARK and several of their colleagues in the Ways and Means Committee of the House.

Mr. President, S. 2576 deals with a problem faced by Medicare beneficiaries—and a lot of a hospitals and physicians—who are being "held up" by the Federal Government.

It deals with a 93-year-old woman in Windom, MN, and an 81-year-old woman in Mountain Lake, MN, and hospital in Crookston, MN—all of whom, right now, are being held up by the Federal Government.

Here's how the Government's scam works.

On December 24 of last year, a 93-year-old woman from Windom, MN, was admitted to her local hospital for