HIGH TECHNOLOGY CRIME INVESTIGATION ASSOCIATION
1999 INTERNATIONAL TRAINING CONFERENCE

- - -

TOWN & COUNTRY RESORT & CONVENTION CENTER
SAN DIEGO, CALIFORNIA

- - -

MONDAY, SEPTEMBER 20, 1999
JANET RENO
9:10 a.m. - 9:40 a.m.

Reported by: Michelle M. Herman, RPR, CSR #10982

- - -

JANET RENO: Thank you, Greg, and thank you very much for your great service. And to you, Mr. Lee, thank you so much. It is wonderful, and I think this is a symbol of what we're all about in this country as we try to address the issues of crime. A Republican DA with a former Democratic DA, that's what it's about. It's not about political rhetoric. It's about common sense in getting the job done, and in that context I salute you all.

I salute you because you're engaged in some of the most important work that law enforcement has ever faced. You are at the cutting edge of one of the most exciting opportunities and one of the greatest challenges that we have faced in America: Do we control the technology, or does the technology control us.

You are proving once again that machines are made by man and humankind. And if we prepare ourselves, if we educate ourselves, we can use these machines, we can use this technology to create some of the most exciting opportunities possible for the American people.

The importance of emerging technologies and the significance of the global information infrastructure stagger the imagination and convert vanity to prayer. This infrastructure, if properly developed and protected, will be used for personal communications, financial transactions, medical care, the development of new intellectual property and a host of other applications. Today economists are giving it credit, the whole information infrastructure, for helping to sustain one of the most prosperous times in our economy and our history.

New technologies allow us to do things that were previously impossible, but they can also be misused in creative ways to threaten both public safety and national security. The same technologies that facilitate lightning fast and ultra-reliable transactions between computers and allow us to use our credit cards all over the world can be misused by criminals looking to obtain those credit cards for fraudulent purposes.

A computer can be used by a man sitting in his kitchen in Saint Petersburg, Russia to steal from a bank in New York. The same technologies that allow us to share photographs of our children and grandchildren across the globe make it possible for others to transmit child pornography to pedophiles.

Of course, child pornography is but one problem. Virtually all crimes can be committed over the Internet, including consumer fraud, hate crimes, economic espionage and terrorism, and the infrastructure itself presents a target for the hacker and for the terrorist. But whatever the case, we are trying to work with you in every way possible.

For example, the Department of Justice has now funded ten state and local Internet Crimes Against Children task forces with eight more soon to be created. These task forces supplement the online investigative programs of the FBI and the US Customs Service.

We have worked large international cases such as Cheshire Cat, a child pornography investigation involving 14 countries and 22 districts in the United States. Next week, we will be actively involved in an international conference on child pornography in

Vienna, Austria, and we want again to be a partner.

With you, we are on the front lines at the state, local and regional level to transmit information, to exchange information and to let you know the latest developments that we have learned of in these conferences.

But it is against this backdrop that we must focus on the future of law enforcement and the unique challenges posed by global networks. But before we go too far into the future in terms of issues that will face law enforcement in cybercrime and in the use of cyber tools, we must concentrate on solving a problem that has plagued us in law enforcement now for too long, and it is now made more problematic by narrow banding and the development of wireless communications.

That problem is how do federal, state and local law enforcement agencies, other first responders, government leaders and citizens communicate together in a secure, reliable way both day-to-day and in emergencies such as Littleton, such as created by Hurricane Floyd, such as in responding to weapons of mass destruction.

I was in Littleton about three days after the tragedy, and again and again law enforcement said: If you can do anything, find a way that we could have communicated effectively during those terrible hours. That is our challenge, to make sure that federal agencies can talk together with state and local, with emergency responders, with fire rescue to make sure that we save lives and that we protect the public.

To that end, the Department of Justice has developed a pilot program. One of the first is here in San Diego, another in Utah, Seattle, and we're looking to South Florida and to Vermont as other instances where we can pilot a project and determine how best to deal with this issue.

The second challenge that I think we all face at whatever level of government is how we recruit and train a sufficient number of people interested in public service, interested in law enforcement who have the expertise necessary to match wits with those that threaten our national security and our public safety.

This is a particularly critical time in that effort, for most of our population doesn't have the expertise either in law enforcement or in computer technology. We are in a situation where industry is paying far more than we can pay in state, federal and local government. We are at a time of full employment.

That is why I salute you, particularly detectives, prosecutors, other people who are concerned, industry representatives who are committed to supporting state and local law enforcement. You are the epitome of public service, and you face one of the extraordinary challenges.

How do we address the issue? First of all, I think we've got to share expertise, share expertise between the different levels of law enforcement, share expertise between industry and law enforcement, share expertise between the academic world and law enforcement, and we need to develop networks that can ensure that be done.

Rather than one institution having to hire its own expert in a certain area, let us share expertise. Let us identify the pockets of expertise across the country. Let us avoid costly duplication and fragmentation that prevents us from understanding the latest developments. If we can plan this together, we can make an extraordinary difference, but we face some challenges.

The technology is constantly changing. There is new equipment. We train agents on Windows 3.1, and a year later they have new machines to run Windows '95, and we have to start all over again.

How do we constantly provide the best in training? The demand for cyber training at this point far exceeds the supply. The Justice Department is actively working to address this need. We have created the national cyber-con training partnership open to any law enforcement organization whose mandate includes electronic crime investigation, prosecution or training.

The partnership is developing training courses, exploring new ways to deliver that training to law enforcement personnel and instituting the trainer programs to increase the supply of available cybercrime teachers. I am committed to that effort; and in the time that follows my remarks, I would like to hear from you as to what we can do to improve that effort.

One of the suggestions that I have made at a federal level is the development of a cyber-corps concept similar to ROTC which would permit people to go to college, develop an expertise for which they had already indicated an aptitude and have the government pay for at least part of their education or for advanced education. We would like to work with you in seeing how that can be promoted. I don't have answers yet in terms of ways to get it done, but this is one of my important projects.

The third challenge, however, that we face is how we put the latest technology in the hands of the people who have the expertise to use it to protect public safety and the national security. It's changing as we speak.

Let's apply the same concept. Let's look at this nation as a whole. Let's say the FBI has this particular technology; this part of government has that. Let's share it because we can electronically communicate and we don't have to have two of this very specialized, very expensive equipment.

The San Diego area has this. It can share that with Los Angeles, with the rest of California. We don't need to have two expensive types of machine. But in other instances, there will be a need for machines at every level and equipment at every level. Let's use our limited resources as wisely as possible and plan a system of sharing in this country that can give you the tools to do the job no matter what the cost.

The President's Fiscal Year 2000 budget requested $350 million to assist state, local and tribal jurisdictions in deploying the latest state-of-the-art technology to fight crime. These monies will enable law enforcement to improve laboratory techniques such as DNA analysis, upgrade criminal history records, establish a global information network and improve police communications.

We are committed to ensuring that law enforcement officers have the tools. We want to work together with congress to provide technology and resources to state and local, to others to avoid the duplication and to ensure the best use of our dollars.

I would like to publicly commend Senator Mike DeWine and Senator Pat Leahy, who have done so much in the development of the DeWine-Leahy legislation to focus on this need that we are discussing today.

But you all here in San Diego are examples that we can cite to show just what is being done and what more can be done if we provide the resources. Here you created the San Diego Regional Computer Forensics Laboratory. I have heard of the development of this laboratory now for a number of years, and I have been touched by this regional multi-agency approach to computer forensics. It's particularly important as computers are increasingly used to commit crime and to store information and communications regarding criminal conduct.

I am convinced that only by pooling regional resources and efforts will we be able to ensure that we can process electronic evidence in a timely fashion limiting the time lag currently suffered in many jurisdictions seeking to obtain an analysis of seized computerized evidence.

Additionally, such coordination will also reduce the legal and factual problems that might arise if different law enforcement authorities use significantly different standards and protocols to seize, secure and analyze computer evidence. Finally, this regional approach will lead to greater training for street officers and agents and will assure the availability of skilled resources in addressing the cases involving electronic evidence.

Simply put, computer forensics is not a discipline that can be developed on an ad hoc basis by individual agencies, departments and jurisdictions. I believe that the San Diego lab will serve as an example for all of us, and I support the development of this and other regional laboratories, as well as the creation and testing of standards to be used regionally, nationally and internationally.

It's not going to help us if there are five different standards for the introduction of evidence around this country and if we can't exchange information so that it can be used and be introduced in another jurisdiction. We have got to develop these forensics standards, and I think this is one of our highest priorities, and we're committed to doing everything we can to work with you in that effort.

Indeed, we have got to look beyond our borders. In 1997 when I hosted the first ever meeting of Justice and Interior Ministers of the G8, the big eight countries, we issued an action plan which calls for, among other things, developing and employing compatible forensic standards amongst the G8 countries. It's not going to do us any good if one of our colleagues across the ocean develops evidence that he thinks is going to be admissible in our courts and cooperates with us in every way possible and then we find that it is not admissible.

One more important point about the San Diego laboratory. I understand that the impetus for the creation of the lab came from the prosecutors, the detectives, the officers who actually work computer cases and who see the problem from a street level perspective. Your solution, the pooling of resources and talent into a regional laboratory, has worked while others have failed.

What is the lesson? The lab has succeeded, I think, because it is a good idea supported and generated by those of you who are on the front line, who work the problem every day, who see what you need in terms of evidence and cases and court time in the real world, not some federal crime problem that we're dealing with when we say, well, we'll get the resources to people when we can. You have the sense of urgency that is so important, and we want to try to respond as well as we can to that sense of urgency.

In all of your communities, I recommend a similar approach. Collect the people who are doing the work, look at what you've got, look at what's available. What do you need? Who can provide it? Does the FBI have some national program that can provide a piece of equipment? Can you obtain monies through a grant from the Department of Justice? Does ATF have a particular piece of equipment that is useful? You've heard of somebody in industry who has been cooperating with law enforcement in a thoughtful way. Can they be of assistance? How do we get the job done without fragmentation, without duplication?

That leads to another challenge. How do we form together a global justice information network that is non-proprietary, that is standards-based, that will permit us to store, access, obtain information in an orderly way from databases across the country that will help us understand what crime problems are being developed in a particular area that we would not have known anything about until we had waited to see the advent of this new problem.

It may be invasion of a meth. distribution system in someplace in Arkansas. It may be the development of a new organization dealing in drugs generally in some other community, but how do we use this information in a global way with reliability, with security to get the job done.

Every detective in this room will tell you that the lifeblood of his or her work is information, information from the snitch, information from the person that the FBI agent interviewed in a totally different manner. But look at what happens in a community where you take FBI 302's, DEA 6's, San Diego Police Department arrest reports and incident reports, San Diego Sheriff's Department's reports, develop them into a database, look at particular areas and plan based on information.

Fifteen years ago, if the same Buick with the battered right fender had been used for 15 different convenience store robberies in 15 different communities in an area, in a county, it might have taken us a very long time to find that out. Now as we develop this capacity, we can find the information so essential to the solution of crimes quickly if we can develop networks that talk to each other.

That leads to the next problem, and I will only touch on it because you will be hearing more about it this week. Even if we develop the best capacity in this country, the creation of global networks means that individuals will increasingly commit crimes across state and national borders. The fellow sitting in the kitchen in Saint Petersburg, Russia is not a figment of my imagination. It is a real situation.

This means that different agencies will have to work together closely in an increasing number of cases. An officer may quickly find himself or herself in the middle of a case with international implications. For example, during the raid of a drug dealer's home, an officer might download data from the suspect's network account only to find out later that the data was stored in a foreign country and the download violated that country's law.

Thus, the Justice Department is actively consulting with our foreign partners on how to handle what has become known as trans-border searches. These discussions are occurring in various fora: The G8, the Council of Europe and the United Nations. Scott Charney will be touching on these issues more this week.

But even if we solve complicated legal issues like trans-border searches, part of our problem will be just the exchange of evidence and information, and the Justice Department is trying to develop partnerships with state and local law enforcement across this country to provide those links that you might not otherwise have access to. Let us know how we can improve those efforts.

One of the biggest challenges that we face in this whole area, however, is encryption. Encryption allows data to be scrambled to protect its confidentiality. The use of encryption is critical. Users of our global information network are to have confidence that their data will be protected and stored in and transmitted over networks.

Indeed, people lose sight of the fact that part of law enforcement's job is to protect privacy. If we do that job successfully, we will enhance public confidence in networks used for communications and commerce, and we will contribute to the remarkable opportunities that this technology provides.

At the same time, however, encryption provides a new and powerful tool for criminals because it provides for unbreakable security for both realtime communications and stored data. Thus, we are gravely concerned that the proliferation of unbreakable encryption could seriously undermine our ability to perform our critical mission.

There is no doubt that court authorized wire taps are among the most successful law enforcement tools used in preventing and prosecuting serious crimes, including organized crime and terrorism. They have been used with great success by law enforcement agencies across the country.

In all of these cases, wire taps were determined by the Department of Justice and others to be absolutely essential to the arrest and prosecution of the targeted individuals and oftentimes to the seizure of millions of dollars with forfeit able assets from the defendants. Occasionally, wire taps are also used in an emergency situation to save lives. For example, emergency wire taps were used in two kidnaping investigations and were directly responsible for saving the lives of the victims.

Encryption can do so much to defeat those efforts unless we figure out solutions. But as crushing as it would be to lose the ability to successfully wire tap criminals, the spread of unbreakable encryption would have a far broader impact. If it becomes commonplace, we will lose our ability to access stored data in all types of cases.

Now, I ask you to let people know just exactly what we're talking about. Many privacy advocates say we shouldn't have access at all, but we now have access to a drug dealer's black book if we can get a search warrant authorized by the court, and the American people would be very upset if we couldn't, through proper processes, get access to the black book.

The drug dealer is taking the black book these days and beginning to put it into the computer; and if we can encrypt computers so that law enforcement can't get into the computer, get into the computer with a search warrant or other authorized warrant of the court, then the American people are going to be upset.

We've got to make clear as we discuss the balance between privacy and public safety about what we can do now, what is necessary both in terms of wire taps and in terms of search warrants for us to have the information we must show the court before we are able to do this.

I think this is important because too many people are confusing the issue. And if we put it in terms of what we do today to protect public safety, I think we can make America appreciate what we're trying to do, and I think we can secure tools that are important in terms of dealing with the issue of encryption.

As encryption proliferates and becomes an ordinary component of mass market items and as the strength of encryption products increases to the point of denying law enforcement access, the threat to public safety will increase exponentially. I can just imagine the day not too far away when every computer sent to the San Diego forensics laboratory has data which is robustly encrypted. What do we do about it?

To support the goal of providing for privacy but ensuring the protection of public safety interests, the administration last Thursday announced a new encryption policy, a balanced approach which will encourage the use of encryption but protect national security and public safety. Essentially, export controls will be simplified, and more encryption products will be easily exportable. This will help secure our networks and prevent crime. Unfortunately, this will make encryption more accessible to criminals. To address that concern, the President has transmitted to Congress the Cyberspace Electronic Security Act, known as CESA.

CESA has three main goals. First, it would protect encryption information held by third parties but provide a legal framework for permitting law enforcement access to such information. Secondly, it would provide a funding authorization of $80 million to fund the FBI's technical support center. This center would provide support to federal, state and local law enforcement when encryption is encountered, and we would work with industry, with the academic world, with state and local law enforcement to provide the latest expertise we could of how to obtain plain text according to constitutional, lawful principles.

This raises one of the most important things that we need to do in the months and years to come, and that is to develop a true, meaningful dialogue with industry and with the academic world so that we have their insight into the latest developments that can provide for privacy while at the same time providing access to law enforcement pursuant to the constitution. Because we will need industry's know-how to get the job done right, CESA provides that such techniques should not be disclosed unless required by the constitution.

There are going to be so many issues that we face. We're going to look back, and we're going to feel as I did when I had my first summer job. I had just graduated from high school. I was on my way to college, and my first summer job was in the Dade County Sheriff's Office. There was a little bitty laboratory, a little bitty fingerprint section, a record section that was on 3 x 5 cards. And I look at the laboratory of the Metro Dade Police Department today, and I marvel at how far law enforcement has come.

If we think we have come that far since the summer of 1956, I think we will look back in ten years and marvel at how far we have come in just ten years. There is so much that we can do to prepare for these new developments if we work together. I look forward to doing that, and I'd like to start that now with you by asking you a question but also throwing the forum open for questions of me.

But my question of you is: If you were the Attorney General of the

United States, how would you improve support for your efforts in the investigation and prosecution of cybercrime and in the utilization of the latest technology and the latest cyber tools available?

I get so many good answers, and I try to take them back to Washington and put them into effect, so let me throw it open now for questions or answers to that question.

- - -

STATE OF CALIFORNIA ss. COUNTY OF SAN DIEGO

I, MICHELLE HERMAN, RPR, CSR #10982 do hereby certify:

That the above proceeding was taken before me at the time and place therein set forth and was taken down by me in shorthand and thereafter transcribed into typewriting under my direction; I further certify that I am neither counsel for nor related to any party to said action, nor in any way interested in the outcome thereof.

IN WITNESS WHEREOF, I have subscribed my name this 21st day of September, 1999.

____

Michelle Herman, RPR, CSR