



UNITED STATES DEPARTMENT OF JUSTICE

Remarks of

THE HONORABLE JANET RENO, ATTORNEY GENERAL

8TH ANNUAL EXECUTIVE LEADERSHIP CONFERENCE

Richmond, Virginia

October 13, 1998

Transcribed from the provided tape for:

The U.S. Department of Justice

P R O C E E D I N G S

ATTORNEY GENERAL RENO: I want to thank the IAC for this wonderful opportunity to talk about how we can built trust, how we can build understanding and how we can work together.

I think this is one of the most exciting times in our history. It is certainly one of the most exciting and challenging times in law enforcement's history. We have an opportunity to build systems and networks that can help us solve crimes in ways that we never dreamed would be possible. But we also have challenges that stagger the imagination and convert vanity to prayer.

How do we face these issues? What do we do?

I am convinced that law enforcement cannot shy away. We must grasp this opportunity. Our national security depends on it. The rule of law depends on it. We cannot turn away. We cannot say we don't understand. But the only way we can meet the challenge is through a partnership between government and industry, between government and the scientists who have made this possible. And we will only be successful if that partnership is built based on certain principles.

First of all, your very existence recognizes that the interconnectivity of the information networks make it essential that law enforcement rely on industry and trust industry. But I think one thing is clear. In all my conversations, at whatever level, with respect to information technology, it is clear that industry and that American business cares deeply about the rule of law, cares deeply about our national security, and in short, we are all in this together. We must trust each other. We must know what we are talking about. And we must be able to communicate with each other in words that people understand.

Now, that includes not just the scientists and the technological experts. That includes lawyers and managers, who sometimes get it confused.

(Laughter.)

ATTORNEY GENERAL RENO: As we talk and as we build trust, one of the first essential principles that we have got to deal with is how we provide security for this tremendous network of information and communications that has been developed. How can we ensure privacy so that I can talk to my friends, thinking that my conversation is not being monitored? How can I ensure privacy, so that the ingredients about my life that have no purpose for anyone else do not end up in one giant database?

How do we achieve the wonderful opportunities that information technology affords us while at the same time adhering to the principles of the Constitution that have been so important to this Nation's history and its very being? How do we work together to solve problems?

Industry should be able to make a profit. And government must realize this. And yet, as it makes a profit, the Nation should be able to develop a cohesive information network, unfettered by fragmentation, duplication and immediate obsolescence that makes the cost of the system so prohibitive?

These are issues that we must confront in law enforcement. We have learned some hard lessons. And, frankly, in some instances, we have learned another. Too often, when I am asked to talk, I am asked to focus on one issue in the whole panoply of issues that we face in information technology. I am going to try to go through the issues that I confront daily, to try to share with you, and hope that I can establish an ongoing dialogue with the IAC about how we solve these problems together.

First is a very simple issue, but very complex. How does law enforcement communicate? We are not talking about fancy technology. We are talking about how do we communicate by radios or by cell phones. In Oklahoma City, it was startling to see the inability of police and State police and Federal officials to communicate with each other.

It becomes imperative that we communicate when we consider the threat of weapons of mass

destruction and how essential it will be for first-responders within communities to be able to communicate and understand the dimension of the problem.

We have an opportunity that has been forced on us in law enforcement. It is an opportunity to -- (off microphone) -- resources. So that I do not look out and see three different radio towers, when one radio tower could do it; that we have an interoperable system, and we build an interoperable system so that we can communicate together; that we develop means of ensuring security; and that we develop the means to talk together.

Now, there are two problems. One, the cost, particularly for State and local first-responders and police officers, particularly in more rural areas and mountainous areas, where the problems of communication become more complex. How do we in law enforcement, in a partnership with State and local communities, develop that system? And how do we do it with limited expertise?

The answer is simple: a partnership with industry, a partnership based on trust, recognizing that we do not have all the answers, but if we sit down together and plan with respect to costs, plan with respect to sharing resources, plan with respect to the interoperability, we can solve the problem.

But it will all be for naught, as we see technology develop, if we cannot preserve some of the fine, old tools of law enforcement. One of the most important tools that has served law enforcement for the last 30 years has been the ability, upon a court order and with very narrow terms, to intercept the communication of another. This tool has been absolutely invaluable to law enforcement in prosecuting drug traffickers, terrorists and kidnapers.

I have personally been involved in a wiretap that probably saved a child's life.

Now, some people say that that is Big Brother watching you. Let me just explain what a wiretap is and what you have to do to get a wiretap. You have to prepare an affidavit, based on solid facts, that you have probable cause to believe that the electronic communication is being used in the commission of a crime and probable cause to believe that you will be able to secure evidence of the commission of that crime.

The prosecutor must present it to the court. In so doing, they must tell the court that there is no other law enforcement method by which that information can be secured, either because it is not reasonably possible or because it is too dangerous to pursue the other law enforcement methods.

We must minimize any innocent conversation overheard on this wiretap, or Title III, as we call it. It is a very strenuous process for law enforcement, but it is critical.

But for five years now, we have grappled with two big issues: how we maintain the capacity to surveil electronically in a digital system, for which Congress has passed what we call CALEA, the Computer Assistance Law Enforcement Act. In this instance, we have tried to work with the industry to see how we can properly implement CALEA.

I think there has been a -- (off microphone) -- together as we should. We have not put ourselves in the other person's shoes, although we have begun to do that. But we have much, much more to do.

The second issue is how we maintain the ability to surveil electronically in the face of strong encryption, while at the same time still providing for the distribution of strong encryption to ensure secure private communication. Both of these goals are very, very important. And we have made progress this past summer on the issue of encryption.

We made it because we sat down and talked with the industry. We made it because we sat down and listened, and listened with a listening ear, and said, let's work together. We recognized that there were no solutions that would guarantee 100 percent of all the answers.

We realized that different solutions would serve different problems. But we realized that we must work together. And we have done so by agreeing to develop a technical support center, in which we bring in the private sector and industry and science, and work together with law enforcement to solve the problems presented by encryption.

These are hard lessons, with more to learn. But the clear implication of everything is that we are all in this together. Industry cares just as much about the national security and the well-being of this Nation as law enforcement. Law enforcement cares that communication should be secure, that it should be private, because that is the best prevention for crime, computer crimes, that we know.

But we now have an opportunity that you have created for us, that just -- (off microphone) -- law enforcement solves crime based on information. The more information it has, the better it can solve a crime.

I used to think when I was a prosecutor in Dade County, wouldn't it be wonderful if I had a big database that I could put every convenience store robbery within a five-county area, trace the battered Oldsmobile with the battered right fender, and pick up the pieces of every crime that Oldsmobile was involved in. Well, now, some good detectives do it either just by manually poring over police report after police report, and some have close to photographic memories. But we all know -- and now we have the opportunity -- to develop in this information age a global information network that presents such opportunities for law enforcement, that we cannot sit still and watch it be fragmented and interoperable.

It is so exciting what you have permitted us to do in terms of detecting at the scene of a crime, taking a DNA sample, immediately transporting it by computer to a databank, immediately making the identification, or excluding an individual from the identification, and immediately giving law enforcement clues that it never had before at such an early time.

We can now take information with respect to terrorists, and combine that into one system, and better understand the situation. And the Oldsmobile is a snap now, thanks to what you have done.

This spring, I met criminal justice practitioners from all levels of government, who were as excited as I am about the possibility and the opportunity of establishing a global criminal justice information network. In their report to me, they identified numerous challenges, including security. If I am going to put my precious information into a system, who do I trust out there?

Well, we can develop means of giving limited access, while at the same time letting people know that this particular police department may have critical information that can be very useful. We can address those problems by what you have developed.

The next issue they presented was privacy. What if the police department decides it is going to develop the greatest database and information sharing possible, and it takes everybody's phone book, bank records, health records? America is going to rise up in arms over that. We have got to address standards of privacy.

They address the issue of the fact that we have incompatible and interoperable systems, the lack of linkages and automation in many areas, the unavailability of information because it is not being captured. Your information network that you are making possible will not be worth very much unless we get the accurate information into the system. And that is one of the problems that we face now.

They spoke of the lack of funding resources at all levels of government, and the lack of sharing information between Federal and State and local entities. Making these problems even harder to solve is that they indicated that there is also a lack of vision regarding future technological possibilities and a lack of understanding, education and resources at policy decisionmaking levels throughout the Federal, State and local systems.

As the Department of Justice continues to work with this group to identify ways of overcoming these challenges, we must all do our part in ensuring that this type of information sharing becomes a reality and not just a dream. Later this year, we will be hearing a report from the IAC, reflecting your assessment of challenges for the global criminal justice information network capability. I am anxious to hear these challenges. And I am more anxious to work together with you to pursue solutions to the problems created by these challenges.

I encourage each of you to see this initiative through. As I have said to some of you before, there is a proliferation of systems, different names, different goals, different objectives, different means of communicating. I have never seen so many information systems as I have seen in the last five and a half years. If we can get them all going in the same direction, if we can get them all going in the same direction while at the same time complying with constitutional safeguards and privacy considerations and security considerations, we are going to have a tremendous tool for law enforcement.

The last issue that I want to deal with is the issue of cybercrime. When a man can sit in a kitchen in St. Petersburg, Russia, and steal from a bank in New York, using his computer, when someone can steal your identity, and then extort from you money because they have stolen your credit card information, when they can extort you in other ways, when they can convey child pornography through the Internet, and they can stalk through the Internet, when they can make boiler rooms more effective on the Internet than ever before, it is imperative that we come together and again look to trust and partnership in determining how we can solve these crimes.

The gun is going to be obsolete in this next millennium. The black book of the drug dealer is now stored on the computer that is encrypted in many instances. Cell phones are tossed away like bubble gum. A tool, again, of the information age.

Law enforcement is sometimes criticized now, again, by the industry, who say, look, I know you all are trying, but your equipment is outmoded and you just do not have the tools necessary to keep up. Or, I know you are trying, but you do not have the expertise that is really necessary. We would like to be able to help you, but we do not know where to start.

We have made some progress. We have developed CART teams, which are forensic teams, across the country, responsible for data recovery and data analysis from the drug dealer's black book, that has become the computer. We have developed the Computer Crime and Intellectual Property Section in the Criminal Division, that has forged new partnerships around the world. And each U.S. Attorney is developing an expertise in their office.

But we have got to do more. We have got to make sure that your clients in the private sectors -- the bankers or others -- report computer crimes inflicted on them. If there is a theft, if there is an intrusion, a banker does not like to report it, because it indicates that the bank might not be as secure as one might like. Or they have developed a pretty good prevention system, and they just want to improve it. Or they are dubious about law enforcement's capacity to do the job.

We have got to develop sufficient trust and confidence so that the bankers and others will be willing to report crime. That is the only way we are going to deter it. If the casual, 18-year-old hacker thinks nobody is going to do anything about it, he is going to hack away. If we are to

develop the information age as we envision it, we are going to have to develop it according to the rule of law. And we are going to have to make sure that the law keeps up with technology.

And so we must work together to solve the technical and legal problems we face. We need to work together in one specific area. We are developing the technological equipment at the Federal level. But police departments and sheriffs offices across the country may not begin to afford some of the sophisticated equipment they need. And we need to work together to develop a comprehensive system in this country of computer forensic systems and equipment that is available on a reasonable and on a national basis for State and local law enforcement, and sharing with the Federal system.

But there will be legal and technical problems. Let me give you an example. Let's talk about the use of digital signatures. Digital signatures allow individuals to electronically sign documents. In a way, this change in the way documents can be signed raises the same issues for us that I talked about in comparing a traditional bank robbery investigation to an investigation of a bank robbery by hacking.

Just like the traditional bank robbery is not like the bank robbery by hacking, the traditional signature is not like the electronic signature. As you all know, the electronic signature is not really even a signature by the conventional definition.

We need to work together in government and industry to be able to determine whether an electronic signature is genuine. If someone falsely files a claim based upon a digital signature, and we seek to prove that the claim was fraudulent, how do we prove in court that the defendant signed the document? After all, in a criminal case, the government cannot ask the defendant if he was the only one to use this encryption key, and whether he kept his encryption key secure. He can simply plead his right against self-incrimination.

The problem is that we cannot conduct a traditional document or handwriting analysis to verify his digital signature the same way we can for a handwritten signature. So how do we evaluate the authenticity of a digital signature? How do we prove that a person's electronic signature was actually made by that person?

Digital signatures have their place. And we have got to ensure their place by working together to ensure that we solve problems just like this. We must challenge ourselves to develop ways that we can apply this technology in a way that meets everybody's needs.

But the problem is greater than one bank theft. Increased reliance on network systems increases our vulnerability to that terrorist, who, with a concentrated attack on our information infrastructure, can bring -- (off microphone). (Off microphone) -- got to help America understand how we deal with this.

The challenge is clearly defined. How does law enforcement accept and meet our responsibilities when we do not and cannot control the technologies and the systems to which the responsibility relates? The answer is, again, a partnership with those who own and operate the systems, and work with them to fulfill our responsibilities.

But how do we develop this partnership? First of all, we had to do more to get our house in order than just developing forensic teams, finding some experts on cyber issues. We had to begin by establishing a center for expertise that I hope will come to represent the best of the government. This center is needed to serve as the government's lead mechanism for responding to computer crimes and attacks against our critical infrastructures. These attacks can include both cybercrimes and acts of terrorism.

On February 27, 1998, I announced the creation of the National Infrastructure Protection Center at the FBI. The Center is a true interagency organization. It includes representatives from the Department of Defense, Treasury, the intelligence community, State and local law enforcement, and other government agencies. It is charged with detecting, preventing and responding to both cyber and physical attacks, including acts of terrorism, on our Nation's critical infrastructures.

The critical infrastructures to be protected by the NIPC include those services -- mostly privately owned -- that are vital to our national security and to our economy. This includes everything from technology to telecommunications to transportation.

The NIPC will also serve to coordinate greater technical assistance and other computer-related cases. It will be a critical mechanism for addressing the national security and law enforcement challenges of the 21st century.

But the government cannot go it alone. Because it does not design, employ, own, or maintain most of the critical network components. Thus, we knew from the beginning of this effort that to protect our Nation's infrastructure, we needed the private sector to be an equal partner in such initiatives as the NIPC. Because much of the relevant expertise in the infrastructures and in industry technology resides in the private sector. We need to ensure direct relationships with private industry, with academic institutions, and with entities such as the Computer Emergency Response Team at Carnegie-Mellon University, and other CERT's across the country.

This will facilitate the two-way exchange of information, and enable us to keep up to date on the latest technologies. This is not only the best way to ensure the protection of the Nation and its citizens, it is the only way.

We are also establishing a national program of information sharing between the government and private industry, called the INFOGARD. For those of you who do not know, INFOGARD

began as a pilot project in Cleveland, established by private sector companies and a Federal enforcement office. It is a system in which industry and government have joined together to share threat and vulnerability information. INFOGARD operates a secure E-mail system and secure Web site to facilitate the two-way exchange of information among its members.

It also provides a vehicle for training, seminars and policy discussions. This fall, the NIPC will expand INFOGARD into a national program, with local chapters in every State, making up one national partnership. The national program is necessary because what happens to a bank in Chicago may be more relevant to a bank in Cleveland than what happens to the power company in Kansas City.

Since cyberspace knows no boundaries, INFOGARD, too, has to transcend physical borders. This type of proactive and close partnership is a significant departure from the way law enforcement has traditionally operated. But the challenges of infrastructure protection require imaginative solutions. And I consider liaison and outreach to the private sector in the development of this Center to be absolutely indispensable to its success. And I would ask you to share with me suggestions as to how I can improve the outreach, what I can do to truly build a partnership with the private sector and the Center.

The system is not going to work unless government has at least sufficient expertise to begin to look at the problem. It does not. The shortage of technology workers with the skills necessary to enable to government to meet these challenges is one of the big problems we face.

We need to make sure that the government recruits and retains the highest quality talent. This personnel problem is of increasing concern due to the increased vulnerability of government systems and communications infrastructure, as well as the growing number of foreign governments and non-state actors that are exploring development of information warfare capabilities.

The demand for quality, high-tech employees will continue to increase, especially as each government department and agency assumes its full responsibility, as required under Presidential Decision Directive 63, to protect its information systems and its physical -- (off microphone).

How can the government recruit the best, even when the talent pool is limited and private sector opportunities abound? First, of course, is that we offer the opportunity for government service. Now, some people these days say, Janet, what are you doing getting cussed at, fussed at and figuratively beaten around the head?

(Laughter.)

ATTORNEY GENERAL RENO: Government service is not that much fun.

(Laughter.)

ATTORNEY GENERAL RENO: These five and a half years have been an extraordinary time for me. I always thought that public service was one of the great callings that anybody could undertake. I have now had the opportunity to visit most of this country, most States. This is such a great Nation. Its people want to be represented and publicly served by good and --

(End of audio.)

(End of transcript.)