REMARKS OF THE HONORABLE JANET RENO

ATTORNEY GENERAL OF THE UNITED STATES

TO THE

NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

(Final)

JANUARY 10, 2000----

Stanford University, Dinkelspiel Auditorium

ATTORNEY GENERAL RENO: Thank you so much, Christine. And to all, I just salute you. I've had a chance now to visit so many different states to watch you in action, Democrats and Republicans, in a bipartisan way, do so much to serve people, not only of your own state, but of this nation. And one of the great points of honor for me has been the opportunity in these last seven years to serve with you. You are great public servants, and very special people, too.

Dean Sullivan, I thank you for your hospitality at this great law school. And, Christine, thank you for giving me this opportunity to speak at what I think is one of the most crucial conferences that I've heard about in a long time.

I come to you today to ask you to join with me to create a strong, permanent network of federal, state and local computer crime experts to do the following:

To share expertise and information technology, to assist each other 24 hours a day, seven days a week, around the clock, to prevent cybercrime wherever possible, and to bring those responsible for such

crime, when it does occur, to justice; To work with industry, the academic world and privacy groups to build trust and to protect our privacy and the Constitutional rights of all Americans; And finally, to ensure that the Internet is a force that brings this world together and builds understanding across peoples and places and time.

I would invite you to meet with me in Washington at your earliest convenience to see how we can work with others -- with police, with prosecutors, with experts -- to forge such a network. For we are facing a moment in history where the decisions we make to confront the challenges of high technology and law enforcement are absolutely critical. These decisions will decisively shape our abilities to cope with crime for all time. The Internet and the revolution in information technology have transformed the world.

The monumental advances in computer software technology over the last ten years, combined with the explosive growth of the Internet, have changed the world forever. With breathtaking speed the Internet has nearly doubled in size every year since 1990. By 2003, the number of Internet users worldwide is projected to be five hundred and two million people.

The Net has brought us splendid tools of wonder. Tools to improve the lives of people all over the world. Tools with which to learn and to teach. Tools with which to communicate with loved ones, with business associates. And as a great means and a great way for government to let its people know what it is doing.

A great example of the power of the Internet is the website for the families of the victims of Pan Am Flight 103. For these families are spread around the globe. But through a website they were able to access the latest developments in the case, reach out to the Office of Victims of Crime to answer their every question, to help them understand the Scottish legal system, and to communicate in private chat rooms with each other, to offer each other unparalleled support and understanding. Despite the great geographical divides that separate these families, the Internet has been a wonderful tool to bring them together and to offer them support at a time when they might otherwise be alone and afraid.

The Internet has provided us with tools to help sustain a vital economy, to generate business, promote commerce. And the volume of e-

commerce is expected so grow from over $100 billion dollars in 1999 to one trillion dollars in the year 2003.

The Net made Christmas shopping a lot easier for an awful lot of Americans this past year. It's promoted telecommuting and an opportunity for people to be with their families at greater measure. And it brings the world together, and it creates new bonds of understanding. It is a splendid tool of wonder.

But there is a dark side, a dark side of hacking, crashing networks, spreading viruses, which cause enormous loss. In a recent survey of Fortune 500 companies by the FBI and the Computer Security Institute found financial losses from computer crime exceeding $360 million from '97 to '99. Of those responding to the survey, 62 percent reported computer security breaches within the last year. And then there is terrorism. Our nation's infrastructures, including the banking system, the stock market, the electricity and water supply, telecommunications network, and critical government services such as emergency and national defense services, all rely on computer networks.

A real world terrorist, in order to blow up a dam, would need tons of explosives, a delivery system, and a surreptitious means with the aid of armed security guards. Cyber terrorists could achieve the same devastating result by hacking into to the control network and opening the flood gates. There is a dark side. A dark side in terms of traditional crime, of threats, child pornography, fraud, gambling, stalking, and extortion.

They are all crimes that, when perpetrated via the Internet, can reach a larger and more accessible pool of victims, and can transform local scams into crimes that encircle the globe. By connecting a worldwide network of users, the Internet has made it easier for wrongdoers to find each other, to congregate, to socialize, and to create an online community of support and social reinforcement for their antisocial behaviors.

And then there is hate and racism, bomb recipes, and insidious communications that tear up the privacy that we hold dear. Made all the more potent by the ease with which they can be accessed, and the concentrated forms that make this information more powerful and more devastating.

How do we ensure the wonderful promise of the Internet? How do we prevail against crime and terrorism on the Internet? How do we protect our privacy and ensure the Constitutional rights we cherish?

None of us can do this by going it alone. In the world of cybercrime, borders mean nothing. Interconnectivity of the information infrastructure means law enforcement, industry and the private sector must work together as never before. As never before in addressing a crime that can have such an impact on all of us. If we come together, if we come together as law enforcement, along with industry and the private sector and privacy groups, we can ensure the promise of the cyber revolution. If we don't, we give the cyber criminals and terrorists an advantage. There is no choice.

Let us all join together to form a strong, permanent network of experts dedicated to preventing computer crime and prosecuting those responsible. Washington likes to have letters for its agencies, with this or that or the other. Why don't we get rid of letters and just call it the Law Net.

I would like to talk about ten steps we must take, I think, to build a law net that can address the problems that we are concerned with. First, as I have indicated, we need to have a 24-hour, seven-day-a-week around the clock network of computer experts who assist each other in tracing and preventing and prosecuting cyber criminals effectively and efficiently. Why do we need this?

With the Internet, the criminal act appears on a computer in a specific location. But the criminal who put that criminal act on the computer could be next door, could be in the next state, could be halfway around the world. We must create and develop the ability to find that criminal and get to where he is in real time.

It doesn't take a master hacker to disappear on a network. For example, a hacker can leave his communications through a series of anonymous remailers, which advertise the fact that they keep no records. Or he can create a few forged e-mail headers with easy-to-use tools available on hacker websites. Or he can use a free trial account or two. Even a novice can effectively hide the trail of his communications and do it quickly.

This is an enormous challenge for law enforcement. For example, if a

cyber stalker in Palo Alto wants to send a threatening e-mail to someone in San Jose, he could easily route the message through hack accounts in New York, Argentina, and Japan before reaching his victim in San Jose.

Investigators in California tracing the message would have to contact service provides and government authorities in Manhattan, Buenos Aires, Kyoto just to track the cyber stalker back to Palo Alto. Tracing such a communication requires not only cooperation by government and industry officials in multiple jurisdictions, it also requires synchronized action and speed.

To combat these new challenges, we must create a system of interdependence, mutual reliability, information sharing, and most of all, integrated, effective connections. We must create an around-the-clock cybercrime network where each participating federal, state and local law enforcement agency designates an expert official to provide immediate assistance with cybercrime investigations to all other agencies in the network.

Questions of jurisdiction will arise; who handles what. I firmly believe in the principles of federalism. And in the principles of the federalism applied here, as in so many other instances, it will be state and local officials who will be pursuing the great bulk of this crime, according to principles of federalism. And we want to work out with you an appropriate understanding of who does what, where, all in the best interests of the people we serve.

The second step of this network involves a challenge for the Law Net, and it involves the development of an interactive secure way for state, local and federal authorities to share the latest techniques, the latest investigative information and intelligence on a secure online clearing house.

For example, if a group of victims complain to a state agency about a website in another jurisdiction, the clearing house website could help locate additional victims and notify authorities in the state where the website was posted.

This would foster cooperation and reduce the duplication of effort. Some existing law enforcement data bases could be used as building blocks for such a clearing house. We have already developed a

nationally coordinated data base in the area of Internet crimes against children. And an Internet fraud complaint center is currently being development by the cooperative efforts of the FBI and National White Collar Crime Center. The complaint center will go gather information about fraud schemes on the Net and forward written investigative reports concerning these schemes to the appropriate state and federal law enforcement agencies.

Let's explore that and make sure that we expand it in every way that is appropriate. And let us share research and development opportunities, both for our immediate needs and for the future. The technology in this area is changing right before our eyes. Unless we are there with the best scientists, the academic world, with industry, preparing for the future, we will find ourselves behind, no matter what we do.

The third area where I believe we have to share is in the utilization of expertise and training. I think this is probably one of the most precious commodities we have: somebody who knows the law, knows investigative techniques, and knows cyber issues.

Our population is catching up to the scientific development of these last 20 years, and the private sector salaries, plus the fact that the entire population has not become computer literate, makes it, as you all well know, very difficult to find and attract people into public service in this area.

That means we must share, must share our recruiting efforts and our training efforts. We must identify and inventory who is an expert in a particular subject matter and make that inventory available so that we don't have to hire 50 experts, but we can hire one for a particular subject to share that with our colleagues around the country.

I think it is imperative, too, that we train managers in how we build this network and how we interrelate together. Lawyers generally are not very good managers. And that makes us sometimes responsible for starting something and not planning it out very well. If we plan this network carefully and prudently, it can last for a long time to come.

I envision the network of contacts that extend from local detectives to the FBI and the National Infrastructure Protection Center, to the

police forces abroad, from county prosecutors and DA's to state AG's, federal computer telecommunications coordinators, or CTC's, to the department's computer crime section and prosecutors in other countries.

We should have a clearing house that provides quick access to these experts. The computer crime and intellectual property section of the Department of Justice has begun to work on this model. They have a national training network of computer crime experts that developed by training assistant United States attorneys from each of the 94 districts across the country.

We call these experts CTC's. They are the resident expert in their district for computer crime cases. On complicated hacker cases, the secretary often will work with this nation-wide network to quickly bring criminals to justice. We want to join forces with the state AG's. And I understand that you have started to lay the groundwork for this effort, and we want to work with you in every way possible.

I know that some of you are well ahead of the curve in addressing this problem with high-tech crime units and among other states; Massachusetts, Michigan, New Jersey, New York, Nevada and Pennsylvania. And I'm told that we can learn a lot from those states. However we proceed, I want to work with you in every way possible to share the expertise.

The next issue is, -- the fourth issue -- we've got to learn how to share our equipment and technology. It makes no sense, if we have a gadget that costs a million dollars, for every state to have to buy the same gadget if we only need it about 25 percent of the time. Let's figure out, in a time where these pieces of equipment are so costly and where they become obsolete right before our eyes, how we can use our dollars as wisely as possible in regionalizing the use of the gadget, the use of the piece of equipment, or making it available nationwide through electronic means so that we use our moneys as wisely as possible. This will require that we develop a plan and a design for how we work together in this network.

Fifth, we must plan for and create regional computer labs that permit us to share the best expertise and equipment in searching computers. This involves not just cybercrime; it involves drug records, financial data, e-mail by co-conspirators. All this evidence is

getting stored on laptops and palm pilots rather than filing cabinets. Sometimes the records to be seized won't be at the search site at all but at a remote server in a commercial network.

Here in California, the shortage of computer forensic experts in Southern California lead to the creation of the first regional computer forensic lab, which involves the participation of federal, state and local computer forensic examiners. This lab was created through a joint initiative with federal, state and local officials, and it is staffed by 16 computer forensic examiners. I believe that this lab is a model that could be replicated in other jurisdictions.

But, again, we must plan. Where should it go? Let's not compete. Let us work together to make sure we serve this nation as a whole. And let us in the process come together and agree on forensic standards which will be the standards applicable throughout the country, wherever possible, for the admission of evidence seized from computers.

Sixth, I think it is important that we explore potential legal solutions. We should explore new and more robust procedural tools to allow state authorities to more easily gather information located outside their jurisdictional boundaries.

I suggest to you that it is time to open a dialogue on whether a new interstate compact should be crafted which respects each state's autonomy, but that commits each signatory state to honoring and enforcing out-of-state subpoenas, search warrants and traffic trace orders.

If cybercrime finds borders meaningless, we're going to have to be prepared to maintain the autonomy of our states, while at the same time developing processes that permit enforcement against those that would ignore boundaries. For example, if Ohio prosecutors need to issue an investigative subpoena for records of a fraudulent website located in Georgia, there is currently no formal procedural mechanism to ensure the enforcement of that out-of-state subpoena.

We need to develop an enforceable legal process. We should also consider possible legislative solutions. One example would be a state law requiring service providers to accept service of process and comply with out-of-state subpoenas, court orders and search warrants.

I understand that California has adopted legislation in this area, and I encourage you to consider whether it would be helpful in your state.

And finally, we would appreciate your thoughts as to whether there is any federal role consistent with principles of federalism and state sovereignty. Would it assist you, for example, if a federal statute allowed states to apply to federal courts for orders with national application.

These are the issues that I think we need to discuss as part of a network in developing answers to enable us to address cybercrime in the most effective manner possible.

I have been speaking of a cooperative network based in this country. But we must look beyond. The seventh issue is international. International borders don't mean anything either. And that is the reason we have reached out to the other ministers of justice, to police authorities in the big industrial nations, the eight big industrial nations of the world, to form a cyber partnership. We have a 24-hour, seven-day-a-week response time in most of these nations now, and it is working. But we have got to do something to move our efforts ahead.

The Office of International Affairs in the Department of Justice has tried to be available to work with you, but the whole concept of the globalization of crime because of the Internet is making their work more and more critical, and they are becoming spread thin.

We must develop means of supporting them so that we can support you with one common goal. The cyber criminal should get the clear message that there is no safe place to hide in this world, and you can't hide just because you are halfway around the world from where the crime was felt here in the United States. We must improve the extradition processes that permit the extradition of nationals -- and I look forward to working with you in that area -- and we must make sure that people understand there is going to be a consequence for a hacking, a consequence for a cyber stalking, a consequence for a terrorist threat.

And some people will say that, how are we going to afford to bring them all the way around the world for trial? We're going to have to

look for new and innovative means of enforcing the law.

And one of the things I think we should explore is the development of video conferencing in which a number of states, I believe, have participated. I know of at least one that permits testimony in another country to be had in the courtroom here through video conferencing.

Right now we must act. People must know that they can not make idle threats across the Internet that terrify students at Columbine High. They must know that there will be consequences for their act. And I believe this network can do much to advance that.

The next issue -- and Christine said she liked this topic a lot -- is dollars. Fighting crime on the Internet is and will continue to be an expensive endeavor. As a former state prosecutor, I am well aware of the great strains on the budgets of state and local law enforcement. Sharing our expertise and cooperation in research and development will help to avoid unnecessary expensive duplication. But the cost of developing and updating technical investigative and prosecutorial expertise and technology will require more than simply sharing the burden.

We must work with our county counsels, state legislatures and Congress to help them understand the importance of this effort, and to help them create a reasonable plan for the nation to provide resources in the most reasoned way possible to fight this effort. We are working through our office of justice programs to do everything we can, along with the FBI, to be a good partner in dollars as well, but we have a long way to go.

An issue of great importance to me is our ninth step that I think we must consider, and that is the issue of privacy. Privacy advocates don't trust us very much. Industry sometimes doesn't trust us very much. And we are going to have to do something about it.

We're going to have to do some outreach, begin some meetings, and let people know that we're all concerned about privacy issues. And nobody likes to pick up the New York Times and see extortion on the front page of the New York Times. Neither the privacy advocate nor the law enforcement person. And we all want one principal goal, and that is that it not happen in the first place. And if we can't avoid that, we

want to make sure that that person is held accountable.

We have to make industry and privacy experts understand that no one wants to allow the invasion of people's privacy. We have to work with them to make sure that the Constitution is upheld; that it is, indeed, a living document; that it is capable of being applied to technology that Alexander Hamilton and James Madison never ever dreamed of.

And finally, the tenth step and way in which I think we can play an important role with our colleagues in education in helping educate our populace, and particularly our children, about the ethical responsibilities of using this powerful tool.

It was first brought to mind when I met with representatives of the telecommunications industries. One leader said, "You know, you've made me think. My 13-year-old daughter knows that she should not steal, that she should not read other people's mail, that she shouldn't go into their bedroom when they're not there and poke around, but I don't think she knows what she should and shouldn't do on the Internet." As part of this network, I think we could be a powerful force in shaping ethical considerations and teaching ethical responsibilities on the net.

As I said at the outset, you all are some of the great public servants that I have worked with. I admire your dedication, your absolute commitment and persistence. I firmly belief that the issues you all discuss at this conference will shape the future of law enforcement indefinitely.

As you confront this challenge, I want you to know that the Justice Department wants to work with you in every way we possibly can as an equal, respectful partner.

I know you have other ideas that come from your firsthand experience with these issues, and I would love to hear them. I'd like to invite you to come to Washington as soon as possible to begin work if you are willing to formally establish this (inaudible due to loud cough from audience).

Our response or our failure to respond, either in this fashion or some other, to these challenges today will determine our ability to

fight crime for many tomorrows to come. We can only do this together. We have shown what we can do together. Let's get started now.