S. HRG. 106–1027

# INTERNET SECURITY AND PRIVACY



## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 25, 2000

**Serial No. J–106–86**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

73–464 WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512–1800 Fax: (202) 512–2250
Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

ORRIN G. HATCH, Utah, *Chairman*

STROM THURMOND, South Carolina
CHARLES E. GRASSLEY, Iowa
ARLEN SPECTER, Pennsylvania
JON KYL, Arizona
MIKE DEWINE, Ohio
JOHN ASHCROFT, Missouri
SPENCER ABRAHAM, Michigan
JEFF SESSIONS, Alabama
BOB SMITH, New Hampshire

PATRICK J. LEAHY, Vermont
EDWARD M. KENNEDY, Massachusetts
JOSEPH R. BIDEN, JR., Delaware
HERBERT KOHL, Wisconsin
DIANNE FEINSTEIN, California
RUSSELL D. FEINGOLD, Wisconsin
ROBERT G. TORRICELLI, New Jersey
CHARLES E. SCHUMER, New York

MANUS COONEY, *Chief Counsel and Staff Director*
BRUCE A. COHEN, *Minority Chief Counsel*

# CONTENTS

## STATEMENTS OF COMMITTEE MEMBERS



## WITNESSES



## APPENDIX

### QUESTIONS AND ANSWERS



### ADDITIONAL SUBMISSIONS FOR THE RECORD

# INTERNET SECURITY AND PRIVACY

**THURSDAY, MAY 25, 2000**

U.S. SENATE,
COMMITTEE ON THE JUDICIARY,
*Washington, DC.*

The committee met, pursuant to notice, at 10:16 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, (chairman of the committee) presiding.

Also present: Senators Leahy, Feinstein, and Schumer.

## OPENING STATEMENT OF HON. ORRIN G. HATCH, A U.S. SENATOR FROM THE STATE OF UTAH

Chairman HATCH. I apologize for being late. I had just a variety of things come up at the last minute. It is just one of those days where you just have to do it, you know.

Let me just say at the outset that the Internet is dramatically changing the way we work, live, play, and learn. According to recent studies, there are over 40 million Internet users today. More than 5 million Americans joined the online world in the first quarter of this year, and roughly 55,000 more Americans join that world each new day.

What is more, more than 3 million Web pages were created every day in 1999, and Web pages in the United States have averaged as high as 1 billion hits per day. Clearly, the Internet is fast becoming the means of choice for Americans to carry out their routine commercial and communication activities.

The Internet's explosive growth promises to impact every aspect of our daily life, as it provides the public with useful and often vital information and literary content immediately at the mere click of a mouse. Internet technology has and will continue to reshape our democracy through its promise to continue to play an important role in educating the population through distance learning and through the general delivery of commerce and information. Additionally, the Internet's ability to allow anyone, regardless of wealth or market power or viewpoint, to deliver his or her perspective for the world to see and hear makes it the ultimate First Amendment enabling technology.

Unfortunately, as recent denial of service and computer virus attacks, as well as the online theft of consumers' credit card information, have made all too clear, the Internet is also becoming an increasingly popular means by which criminals, including terrorists, commit crimes and attack our Nation's critical infrastructure.

Americans are concerned that the Internet not become a haven for anonymous criminals who can remain beyond the reach of law

enforcement. At the same time, however, as Americans spend more of their time on the Internet, they are also legitimately concerned about the ability of Web sites, both government and commercial, to track their digital steps. Consumers must be assured that personally identifiable information that is collected online is afforded adequate levels of protection. How do we do so without chilling the development of new technologies or the expansion of the marketplace?

When we talk about "privacy on the Internet," we mean the level of protection that Web sites operators accord Internet users' personal information. The basic issue revolves around giving Internet users notice about what personal information will be collected by government and commercial Web sites when they visit the site and how it will be used. Most Web sites collect and sell personal information through online registrations, mailing lists, surveys, user profiles, and order fulfillment requirements.

Internet security refers to the extent to which Web sites are vulnerable to unauthorized intrusions or attacks by ill-motivated persons. So far, many of the attacks have been carried out by pranksters trying to make a point or achieve a measure of notoriety. There have been, however, several instances where a Web site has been broken into and the intruder has stolen sensitive credit card information from the site. Internet security is, of course, a natural complement to the privacy issue. Both are essential to ensuring the integrity of the Internet.

The task confronting us is how to develop and implement public policies that advance each of these interests. While some believe these goals are in hopeless conflict, I firmly believe that properly calibrated laws can simultaneously protect the Internet from criminals and terrorists, respect the legitimate privacy interests of Americans, and allow the Internet to flourish free from burdensome regulation.

The Internet Integrity and Critical Infrastructure Protection Act of 2000, which I recently introduced together with Senator Schumer, strikes the appropriate balance. It will not prevent bad actors from misusing the Internet, but it will provide much needed resources and investigative tools to government agencies charged with protecting us against Internet crime and update our computer abuse laws to help deter and prevent such activities. The bill accomplishes these ends without undermining the growth of the Internet or lessening legitimate privacy interests.

The bill also will assure consumers with respect to their personally identifiable information that is collected by Internet companies. The bill requires that a Web site provide customers with a notice of its practice and allow customers the opportunity to prevent their information from being sold to third parties. This approach provides for privacy protection without imposing a burdensome regulatory framework and without a Federal bureaucracy overseeing the various business practices of Internet companies. The bill puts in place general statutory rules, but leaves industry free to determine how best to comply with them.

It is imperative that steps are taken, preferably by industry, but by government where necessary, to protect the integrity, security, and privacy of the Internet. By introducing this legislation, how-

ever, I am not suggesting that government must play a role in ensuring Internet integrity and privacy. Indeed, I would prefer to encourage private sector solutions within the industry, and I hope to hear your thoughts on what is being done to develop these non-governmental solutions.

Now is the time for the various interests—private industry, law enforcement, other government agencies, and privacy and consumer groups—to come together and formulate policies that will help us to realize the promise of the Internet.

Well, we are grateful to have a variety of witnesses here today. Let me introduce our first panel of witnesses. First, we have Michael Vatis of the Federal Bureau of Investigation. Mr. Vatis is the Director of the National Infrastructure Protection Center here in Washington, DC.

Our next witness is James K. Robinson, the Assistant Attorney General for the Criminal Division at the Department of Justice. Mr. Robinson is accompanied by Ms. Martha Stansell-Gamm, who is the Chief of the Computer Crime and Intellectual Property Section at the Department of Justice.

So we are happy to have both of you here today, and we look forward to taking your testimony at this time. Mr. Vatis, we will turn to you first.

**PANEL CONSISTING OF MICHAEL A. VATIS, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION, U. S. DEPARTMENT OF JUSTICE, WASHINGTON, DC; AND JAMES K. ROBINSON, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U. S. DEPARTMENT OF JUSTICE, WASHINGTON, DC, ACCOMPANIED BY MARTHA STANSELL-GAMM, CHIEF, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U. S. DEPARTMENT OF JUSTICE, WASHINGTON, DC**

**STATEMENT OF MICHAEL A. VATIS**

Mr. VATIS. Mr. Chairman, thank you very much for inviting me this morning to discuss cyber crime in general, and S. 2448, the Hatch-Schumer bill in particular.

As you noted in your opening remarks, cyber crime is clearly on the rise. That fact is borne out in not only anecdotal accounts in the news media, but also in the recent Computer Security Institute and FBI survey of private companies which showed that most companies have had some sort of computer intrusion or denial of service in the last year. It is also borne out by the marked increase in the FBI's caseload involving computer intrusions and other sorts of cyber crime. So this is clearly a growing problem that we need to address.

The I Love You or Love Bug virus that hit companies and individuals around the world earlier this month is really only the latest instance of destructive viruses that coarse through the Internet. Last year, we saw the Melissa virus wreak similar havoc around the world, and the Explorer Zip virus as well.

Earlier this year, in February, we also saw distributed denial of service attacks on critical e-commerce sites, and also Government agencies, that had the effect of knocking those sites off line for at

least several hours. Now, that may not be a big deal for somebody who is merely posting a personal Web site with personal information on the Internet. But for a company that is engaged in online commerce or e-commerce, that could be a critical thing and cause significant economic damage.

But viruses and distributed denial of service attacks are only one part of the pie that we are dealing with. We are also seeing, as you mentioned, numerous intrusions that go beyond pranksters or people just merely trying to show their hacking skills, but involve organized criminal activity to steal private information, proprietary data from companies about high-tech developments, credit card information, et cetera.

In addition, we need to keep in mind that this is not just a crime problem. It is also very much a national security problem because of the potential for foreign intelligence services, foreign terrorist groups, and foreign military organizations to use these same sorts of tools to steal sensitive information from government agencies or to disrupt or deny service to critical infrastructure systems, which would have a broad-scale debilitating impact on our economy and our national security.

So we are attempting in our efforts to deal with this problem to look at the whole spectrum of threats, ranging from the insider at a company who engages in hacking as a means of getting revenge against his employer or an individual teenage hacker, all the way to information warfare at the opposite end of the spectrum, and a whole myriad of challenges in between those things.

The National Infrastructure Protection Center is an interagency organization located at the FBI that is attempting to do several things. On the one hand, we are attempting to gather information from all potential sources about the threat. That includes intelligence sources, law enforcement sources, and information provided to us voluntarily by private companies, so we can understand the full panoply of threats and have a picture of what is going on out there in the world in real time so that we can issue alerts and warnings and analyses to the people who are potential victims of these sorts of attacks.

On the other hand, we are also trying to improve our capability to respond effectively to attacks that do occur, whether they be criminal attacks or national security attacks. And because of that broad spectrum of threats that we deal with, we work very closely with agencies from the intelligence community, from the Defense Department, from other law enforcement agencies, and most importantly from the private sector to ensure that we have as much information as possible.

You mentioned how critical outreach to the private sector is. We fully agree with that, and as a result we have several outreach ventures, including our InfraGard and our Key Asset initiatives which are described in my formal written testimony in full. But they basically involve our efforts to develop liaison relationships with private companies so that we can give them information that we have that is relevant to their ability to protect themselves, and they can give us information that they have which might be relevant to our ability to investigate crimes and possibly deter them before they occur.

With regard to the Hatch-Schumer bill, I will defer to Mr. Robinson for the bulk of the FBI and the Department's remarks on that, but I will say a couple of things in particular. We think the bill is an extremely useful advance in our ability to deal with this problem, particularly in the area of resources.

It is my view that the number one thing we need right now is additional resources to deal with this fast-growing problem. Therefore, section 402 and section 109 are particularly welcome to us, in that they would give us additional resources both to do investigations and the forensic examination of computers.

We are also very much in favor of the increased penalties that are in the statute, and the elimination of the $5,000 threshold for Federal jurisdiction, because both of these things would provide additional deterrence to would-be criminals.

I should mention there is one item in the bill that does cause us some concern, and that is the expansion of Secret Service jurisdiction for various areas of computer crime. When Congress first passed the Computer Fraud and Abuse Act in 1986, it set out careful delineation of the relative jurisdiction of investigative agencies which we think has worked well and has prevented confusion.

The item in the bill that would do away with that delineation causes us concern because we think it creates the potential for confusion particularly in the area of electronic espionage, which we think should properly remain within the jurisdiction of the FBI, which has really the sole jurisdiction to investigate espionage in general right now.

Then I would point out one thing that we think is missing that we would like to see added to the bill, which is the creation of a nationwide pen or trap and trace order so that one Federal court would have the ability to issue one order that would follow a communication regardless of how many jurisdictions it went through. Right now, we are in the position of having to get numerous court orders to follow a single communication because an electronic or wire communication can pass through numerous jurisdictions at once. We know that provision is in S. 2092, but we would like to see that also added to S. 2448 because we think that is critical to our ability to quickly pursue an investigation.

So we look forward to working with your staff on these and other suggestions that we have with regard to the bill, and I thank you again for inviting me here today.

[The prepared statement of Mr. Vatis follows:]

PREPARED STATEMENT OF MICHAEL A. VATIS

Good morning, Mr. Chairman, Senator Leahy, and Members of the Committee. I am grateful for this opportunity to discuss cybercrime in general and S. 2448, the Hatch-Schumer bill, in particular.

Last month the Computer Security Institute released its fifth annual "Computer Crime and Security Survey," The results only confirm what we had already suspected given our burgeoning case load: that more companies surveyed are reporting illegal intrusions, that dollar losses are increasing, that insiders remain a serious threat, and that more companies are doing more business on the Internet than ever before—and are thus vulnerable to the rising tide of cyber crime.

The statistics tell the story. Ninety percent of respondents detected security breaches over the last 12 months. At least 74 percent of respondents reported security breaches including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, or denial of service attacks. Many companies experienced multiple attacks; 19% of respondents reported 10 or more in-

cidents. Information theft and financial fraud caused the most severe financial losses, estimated by the respondents at $68 million and $56 million respectively. The losses from 273 respondents totaled just over $265 million. Notably, this survey does not include harm caused by recent destructive episodes such as the Distributed Denial of Service attacks on e-commerce sites in February, and the "ILOVEYOU" or "Love Bug" virus earlier this month. Unfortunately, we should expect that the results of next year's survey will show a continuing upward trend in the damage caused by cyber crime.

Over the past several years we have seen a broad spectrum of computer crimes ranging from defacement of websites by juveniles to sophisticated intrusions that we suspect may be sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area has greater consequences for national security, public safety, and the economy than the defacement of a web-site. But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A website hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. And a destructive virus that disables a company's email server or forces it to disconnect from the Internet can significantly disrupt business operations. The harm caused by the Distributed Denial of Service attacks in February and the "ILOVEYOU" virus this month are only the most recent examples of the magnitude of this problem. The fact is that far more cyber crime occurs that the public never hears about. Accordingly, it is imperative that Congress and the Executive Branch work together to ensure that we have the legal authorities, the programs, and the resources we need to investigate, and, ultimately, deter these sorts of crimes.

## "ILOVEYOU" VIRUS

Let me take a minute to update the committee on the ILOVEYOU virus (or worm) matter. The NIPC first learned of the virus on May 4, 2000 at 5:45 a.m., when an industry contact called the NIPC Watch to inform it of the virus. The Watch's standard procedure when informed of a virus is to verify the report and determine its potential significance by checking various law enforcement, intelligence, private sector, and "open" (e.g., media) sources. There are on average over 30 new viruses disseminated every day, with over 50,000 known viruses in existence overall, and most do not warrant a public warning because they are not terribly damaging, do not propagate easily, and/or are detected by existing anti-virus software. Accordingly, it is important for us, as well as for private sector computer response entities, to assess virus reports to ensure that the reports are credible and that a virus is significant enough, in terms of its destructive impact and the speed and breadth of propagation, to warrant a public warning. Creating an unnecessary panic or perpetuating a virus hoax could be just as damaging as a real virus if it causes people to unnecessarily disconnect from the Internet or shut down email.

Unfortunately, there was not a great deal of information available on the new virus early on May 4. Nevertheless, by 7:40 a.m.—less than two hours after we had received the initial report—the NIPC had obtained sufficient information to verify the initial report and assess the virus. We then immediately notified the Federal Computer Incident Response Capability (FedCIRC), which is responsible for assisting government systems administrators in addressing computer network vulnerabilities. This notification was made by telephone because of the urgency of the situation and the need to make immediate contact. FedCIRC then began notifying other government agencies, completing the process by approximately 9 a.m. The NIPC also telephonically notified the Computer Emergency Response Team-Coordination Center at Carnegie Mellon University, which assists private sector systems administrators. This process was the most expeditious means available for reaching a broad audience, while we continued to seek out and assess additional information. Subsequently, the Watch loaded the alert into our website, so that it was accessible to the general public, and sent the alert our directly to thousands of private companies and state and local law enforcement agencies. The Watch then continually provided updates on the virus and its many variants.

To date, the NIPC has published 18 alerts on variants of the ILOVEYOU virus as they are identified. We have also issued an alert on a new, more destructive virus, dubbed the "New Love.vbs" virus. The "New Love" virus deletes a much broader range of files than did the variants of the ILOVEYOU virus. In addition,

this virus is "polymorphic," in that each new dissemination of it comes in a new guise and with slightly different code, which makes it harder both for human recipients and anti-virus software to detect. The NewLove.VBS variant uses the filename of a file that a user has recently been working on, and places that filename in the subject line of the email transmission. The recipient may thus think that he has been forwarded a file from a known associate. When the attachment is opened, this worm can damage or delete most or all files not currently in use. It can also transmit itself to a new group of victims taken from the current victim's email address book. Each wave to emails will have a different subject line taken from a filename that the current victim has recently been working on. In addition, each wave will contain slightly altered code in the attachment, in order to try to evade anti-virus software updated to address earlier iterations of the virus.

The NIPC began issuing alerts on the New Love virus at approximately 2 a.m. on May 19. Fortunately, although this virus is more destructive than the ILOVEYOU virus, it has not propagated nearly as quickly, in part because of early warnings and the heightened awareness by users after the ILOVEYOU episode of the need to take caution in opening email.

In addition to issuing alerts, the NIPC has been coordinating and supporting the FBI investigations into the ILOVEYOU virus and some of the variants. Notably, the FBI's New York office was able to obtain leads on the ILOVEYOU virus very quickly, and contacted authorities in the Philippines within a day of the virus' spread. FBI agents from the United States as well as the FBI Legal Attache in Manilla are working closely with the Philippine National Bureau of Investigation. Some of the officers assigned to the case there are ones we have trained as part of our international outreach program.

*Initiatives to fight cyber crime*

Since its creation two years ago, the NIPC has moved aggressively to address the growing threat of cyber crime through several coordinated efforts. The NIPC serves as a focal point for the Federal Government's efforts to detect, assess, warn of, and respond to cyber attacks. To accomplish its goals, the NIPC is organize into three sections:

The Computer Investigations and Operations Section (CIOS) is the operational response arm of the Center. It supports and, where necessary, coordinates computer investigations conducted by FBI field offices throughout the country, provides expert technical assistance to network investigations, and provides a cyber emergency response capability to coordinate the response to a national-level cyber incident.

The Analysis and Warning Section (AWS) serves as the "indications and warning" arm of the NIPC. It provides tactical analytical support during a cyber incident, and also develops strategic analyses of threats for dissemination to both government and private sector entities so that they can take appropriate steps to protect themselves. Through its 24/7 watch and warning operation, it maintains a real-time situational awareness by reviewing numerous governmental and "open" sources of information and by maintaining communications with partner entities in the government and private sector. Through its efforts, the AWS strives to acquire indications of a possible attack, assess the information, and issue appropriate warnings to government and private sector partners as quickly as possible.

The Training, Outreach and Strategy Section (TOSS) coordinates the vital training of cyber investigators in the FBI field offices, other federal agencies, and state and local law enforcement. It also coordinates outreach to private industry and government agencies to build the partnerships that are key to both our investigative and our warning missions. In addition, this section manages our efforts to catalogue information about individual "key assets" across the country which, if successfully attacked, could have significant repercussions on our economy or national security. Finally, the TOSS handles the development of strategy and policy in conjunction with other agencies and the Congress.

The broad spectrum of cyber threats, ranging from hacking to foreign espionage and information warfare, requires not just new technologies and skills on the part of investigators, but new organizational constructs as well. In most cyber attacks, the identity, location, and objective of the perpetrator are not immediately apparent. Nor is the scope of his attack—i.e., whether an intrusion is isolated or part of a broader pattern affecting numerous targets. This means it is often impossible to determine at the outset if an intrusion is an act of cyber vandalism, organized crime, domestic or foreign terrorism, economic or traditional espionage, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to gather information from the victim sites and intermediate sites such as ISPs and telecommunications carriers. Under our constitutional system, such information typically can be gathered only pursuant to criminal investigative

authorities. This is why the NIPC is part of the FBI, allowing us to utilize the FBI's legal authorities to gather and retain information and to act on it, consistent with constitutional and statutory requirements.

But the dimension and varied nature of the threats also means that this is an issue that concerns not just the FBI and law enforcement agencies, but also the Department of Defense, the Intelligence Community, and civilian agencies with infrastructure-focused responsibility such as the Departments of Energy and Transportation. It also is a matter that greatly affects state and local law enforcement. This is why the NIPC is an interagency center, with representatives detailed to the FBI from numerous federal agencies and representation from state and local law enforcement as well. These representatives operate under the direction and authority of the FBI, but bring with them expertise and skills from their respective home agencies that enable better coordination and cooperation among all relevant agencies, consistent with applicable laws.

In addition to the activities at NIPC headquarters, the NIPC has established a National Infrastructure Protection and Computer Intrusion (NIPCI) Program in the FBI field offices across the nation. Currently 16 field offices have computer intrusion squads, while other offices have at least one agent working computer intrusion and infrastructure protection.

Much has been said over the last few years about the importance of information sharing. Since our founding, the NIPC has been actively engaged in building concrete mechanisms and initiatives to make this sharing a reality, and we have built up a track record of actually sharing useful information. These efforts belie the notions that private industry won't share with law enforcement in this area, or that the government won't provide meaningful threat data to industry. As companies continue to gain experience in dealing with the NIPC and FBI field offices, as we continue to provide them with important and useful threat information, and as companies recognize that cyber crime requires a joint effort by industry and government together, we will continue to make real progress in this area.

The effort to protect the nation's critical infrastructures and deter computer intrusions, however, requires close cooperation with the private sector and with state and local law enforcement. The NIPC is pursuing several significant outreach efforts to the private sector. Our Key Asset Initiative (KAI) is focused specifically on the owners and operators of critical components of each of the infrastructure sectors. It facilitates the response to threats and incidents by building liaison and communication links with the owners and operators of individual companies and enabling contingency planning. The KAI began in the 1980s and focused on physical vulnerabilities to terrorism. Under the NIPC, the KAI has been reinvigorated and expanded to focus on cyber threats and vulnerabilities as well. The KAI currently involves determining which assets are key within the jurisdiction of each FBI Field Office and obtaining 24-points of contact at each asset in cases of emergency. Eventually, if future resources permit, the initiative will include the development of contingency plans to respond to attacks on each asset, exercises to test response plans, and modelings to determine the effects of an attack on particular assets. FBI field offices are responsible for developing a list of the assets within their respective jurisdictions, while the NIPC maintains the national database. The KAI is being developed in coordination with DOD and other agencies. Currently the database has about 2400 entries.

A second outreach initiative is InfraGard. This is actually an initiative that was created by private companies and academic institutions that wanted to get together and share information about threats and vulnerabilities with each other, and with the FBI. A vital component of InfraGard is the ability of industry to provide information on intrusions to the local FBI field office and to the NIPC using secure e-mail communications in both a "sanitized" and detailed format. The local FBI field offices can, if appropriate, use the detailed version to initiate an investigation; while NIPC Headquarters can analyze that information in conjunction with other information we obtain to determine if the intrusion is part of a broader attack on numerous sites. The NIPC can simultaneously use the sanitized version to inform other members of the intrusion without compromising the confidentiality of the reporting company. The key to this system is that whether, and what, to report is entirely up to the reporting company. A secure web site also contains a variety of analytic and warning products that we made available to the InfraGard community. Alerts can also be sent directly by the NIPC Watch to InfraGard members.

Another initiative is a pilot program we have begun with the North American Electrical Reliability Council (NERC) to develop an "Indications and Warning" System for cyber attacks. Under the pilot program, electric utility companies and other power entities transmit cyber incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC warning, alert, or advisory is

warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. It is our expectation that the Electrical Power Indications and Warning System will provide a mode for the other critical infrastructures. We are currently working with industry on a Indications and Warning model for the telecommunications sector.

With regard to state and local law enforcement the NIPC has sponsored computer investigations training for state and local investigators, in addition to FBI and other federal investigators. In the last two years we have trained hundreds of FBI and other-government-agency students in NIPC sponsored training classes on network investigations and infrastructure protection. The emphasis for 2000 is on continuing to train federal personnel while expanding training opportunities for state and local law enforcement personnel. During FY 2000, we plan to train approximately 740 personnel from the FBI, other federal agencies, and state and local law enforcement. As of April, 2000 we had already trained 540 students in FY 2000. The NIPC also has held international computer crime conferences and offered cyber crime training classes to foreign law enforcement officials to develop liaison contacts and bring these officials up to speed on cyber crime issues.

In addition, in its role under Presidential Decision Directive (PDD) 63 as the lead agency for the "emergency law enforcement sector," the NIPC has been working with state and local law enforcement to develop a plan to protect that sector from cyber attack and reduce its vulnerabilities. As part of that effort, the NIPC's alerts and warnings are regularly sent to state and local law enforcement agencies via the National Law Enforcement Telecommunications System (NLETS).

All of these efforts are critical to our ability to build a partnership across government agencies at all levels, and between the government and private sector. They have already borne fruit in that we have seen an unprecedented level of cooperation and information sharing to address cyber threats. But much work remains for us to expand our base of contacts and build a system that allows for speedy reports by private companies and government agencies, so that we get the earliest possible warning of developing threats, and that permits expeditious alerts and warnings by the NIPC to government agencies, private companies, and the public, as appropriate.

*The Hatch-Schumer bill*

With regard to S. 2448, the Hatch-Schumer bill, I will generally defer to Assistant Attorney General Robinson, and confine my comments to only a few items. Let me say at the outset, however, that we are very pleased that in a year that has seen some of the most destructive attacks ever on the Internet, Congress, and in particular the Senate Judiciary Committee, is acting to strengthen the computer intrusion laws and enhance our ability to fight computer crime, while protecting privacy rights.

While some of the legislative changes effected by the bill (and others not in the bill, which I will mention below) are important, it is our view that the most pressing need right now to enhance our ability to fight cyber crime is additional investigative capabilities. Unless we have a sufficient number of trained cyber investigators and analysts, and state of the art equipment to help analyze and process data, we simply will not be able to do our job, and fulfill our mission under PDD 63, adequately. For this reason, we welcome section 402 of S. 2448, which authorizes the appropriation of additional resources.

Similarly, we welcome the effort in Section 109a of S. 2448, to develop a greater capability at the federal, state, and local level for law enforcement to address the burgeoning load of computer forensics. This forensic work is critical not only in what we commonly refer to as "computer crime" (meaning crimes in which criminals use computers as tools to attack other computers to steal money or information, undermine the integrity or data, or deny or disrupt service) but also in more traditional investigations involving organized crime, narcotics trafficking, espionage, terrorism, child pornography, white collar crime, etc. Further, as the frequency of encounters with encryption increases, it is essential that the FBI be capable of utilizing techniques to deal with encryption products. For as the world continues to do more and more business on-line, more and more evidence of crime is being found on computers, necessitating the work of specially trained forensic examiners to produce critical evidence.

The FBI believes that there is and necessarily will be a logical synergy between the missions and functions of this enhanced national capability and the Regional Computer Forensics Labs as part of a successful, multi-layered, pyramidic cybercrime strategy. In order to realistically achieve the maximum allocation of pre-

cious technical and personnel resources, as well as achieve economies of scale, we support this enhanced technical support capability.

In addition to these provisions that would increase our investigative capabilities, S. 2448 would effect changes in the Computer Fraud and Abuse Act that would enhance our ability to investigate computer intrusions, denial of service attacks, and propagation of computer viruses and, ultimately, provide a greater deterrence to those who might engage in computer crime in the future. In particular, we support provisions that make the penalties match the seriousness of the damage caused by large scale computer crime. The current penalties provide inadequate deterrence, and send the inappropriate signal that a computer crime that could cause millions or even billions of dollars of damage is not treated seriously by the Federal Government. We also support revision of the $5,000 proof of damage provision; S. 2448 would make federal jurisdiction attach to the nature of the computer intrusion rather than the dollar value of damage. We have seen many instances where the damage is difficult to determine in dollars, but where the crime is extremely serious based on the nature of the systems that were affected or the potential damage that the criminal could have caused with a mere tap on the keyboard.

*Additional legislative changes*

There are additional legislative changes not in S. 2448 that would assist law enforcement in the investigation of computer crimes. Many of the present statutes that are used in the investigation of computer crime were written prior to the widespread use of personal computers, desktop publishing, and the Internet. These drafters of these laws surely did not intend that criminals simply using new technology could hide their activities from law enforcement and escape prosecution. The Pen Register/Trap and Trace Statute is one significant example.

As the Director testified on March 28, 2000 on S. 2092, the FBI supports provisions of S. 2092 that renders the language regarding pen traps and traces technology neutral. This is especially critical in light of changing technology. Even the terms "pen register" and "trap and trace" are of limited significance today and harken back to a time when telephone companies would actually attach a physical device to a telephone line to implement these court orders. Today, few phone companies attach a physical device to an individual telephone line. It's critical that our investigative laws keep pace with the evolving technology utilized by criminals.

*Conclusion*

The last couple of years have witnessed a series of increasingly destructive attacks on our government and commercial computer networks. In 1998, young hackers from California and Israel were able to penetrate numerous Department of Defense computers and gain "root" access, meaning they had the capability to shut the systems down or steal or alter important information. In 1999, the Melissa Macro Virus caused at least $80 million in damage and affected networks and systems all over the world. In 2000, Distributed Denial of Service attacks took some of the most popular e-commerce sites off-line for several hours, causing enormous losses in terms of lost business opportunities and repair costs. Most recently, the ILOVEYOU virus impaired government and commercial systems across the globe by jamming e-mail servers and erasing computer files. All of these events, and the many more that don't make the front pages of newspapers but may be at least as significant in terms of their impact on our economy or our national security, all demonstrate the urgent need for greater resources for law enforcement to address these problems and for changes to the applicable laws to enhance our investigative capabilities and provide added deterrence. S. 2448 is a welcome step in our battle against cybercrime. We look forward to working with the committee staff to provide more detailed suggestions on this important legislation. Thank you.

The CHAIRMAN. Thank you, Mr. Vatis.

Let me turn to Senator Schumer, who has a short statement he would like to make as a prime cosponsor of this bill.

## STATEMENT OF HON. CHARLES E. SCHUMER, A U.S. SENATOR FROM THE STATE OF NEW YORK

Senator SCHUMER. Well, thank you, Mr. Chairman. I want to thank you for your leadership on this, as on so many other issues, and for being such a fine person for a new Senator to work with, which I appreciate very, very much.

The CHAIRMAN. Thank you very much.

Senator SCHUMER. Mr. Chairman, I appreciate the opportunity to make a statement. I am in the Banking Committee and here on two issues I care about, so I will be shuttling back and forth the whole morning.

Mr. Chairman, let's face it, we are in a brave new world. In 1993, there were 13 non-government sites on the World Wide Web. Today, there are 14 million. And as the Web has mushroomed, Internet crime has quickly and quietly become a clear and present danger to our national security, our economy, and all our lives.

In 1996, the cost of Internet crime was about $100 million. In 1998, the number tripled, and now a single computer virus, the I Love You virus, can cause on its own financial losses in the billions. The denial of service attacks a few months ago and the I Love You virus show how easy it is to cripple the most prized computer networks around the globe, and how helpless law enforcement can be in catching those responsible. Up to now, it seems those who have caused damage are doing it almost for sport. What is going to happen when someone with far more nefarious purposes starts to do this?

Mr. Chairman, there are multiple causes of this problem. First, most computer systems are not sufficiently secure, and security was usually a relatively low priority in the development of computer software and Internet systems. Second, hacking is still considered more of a prank than a crime, even though hacking could cost lives or billions of dollars to the economy.

Third, our laws, even our computer laws, are set up for a world that travels at sub-sonic speed, while hacking crimes and computer viruses move at the speed of light. We have fallible systems vulnerable to hackers who are viewed with bemusement, and laws that make it difficult to apprehend them.

And we are constantly learning. For instance, one major problem we face with computer crime is the failure of many companies to report hacking incidents. Until recently, I assumed this was because companies thought their businesses would be hurt and their vulnerabilities exposed. But I have recently learned an additional reason. Apparently, it is part of the hacker ethic that if a company reports its incident, then it is open season in the hacker community against that company.

I have also learned recently of a growing number of Net denizens who are helping law enforcement by serving as private Net detectives. Maybe it is time we started thinking about how to harness this excellent resources that could be the next wave of community policing.

Mr. Chairman, clearly this new world of computer crime requires new study and new solutions. And as the Net goes wireless, we may need even new, new solutions. At the very least, I am convinced that taking on computer crime will be tricky, requiring far-reaching and complex solutions that, among other things, require significant cooperation from foreign governments. International borders are not even speed bumps on the information superhighway.

And we shouldn't fool ourselves into thinking Congress can alone solve this problem or do so right away. With that said, I think there are some common-sense changes we can make. They are em-

bodied in the bill that Senator Hatch and I have introduced, and I won't go over them, but the comprehensive bill facilitates the apprehension, prosecution, and punishment of computer criminals. In addition, Senator Kyl and I have introduced S. 2092 that for the first time provides law enforcement with nationwide trap and trace authority.

The bottom line is that the creation of a more secure environment in cyberspace is good for everyone except criminals. The question is whether we can come up with appropriate solutions that will deter and punish crime without impinging on the rights of individuals and slowing down the booming growth in the Net.

Mr. Chairman, I think the bill we have introduced is a good start, and I appreciate your holding hearings on it. I also thank my ranking member, Senator Leahy, who is just walking in, although I was mentioning him before I saw that, for all this good work on this issue.

Thank you.

The CHAIRMAN. Thank you.

Senator Leahy, do you have a statement you would care to make?

**STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT**

Senator LEAHY. I do, Mr. Chairman, and I will keep it brief.

I think that computer-related crime really is a major challenge for law enforcement. I think of what happened with the Love Bug. We ended up worried all last year about the Y2K problem, which turned out to be a big yawn because of work done here, but also in countries that even did very little or any work it was not much of a problem.

Now, with the Love Bug, we are talking about billions of dollars of damage. I know how many problems it caused my own office, and efforts to clean and purge files to make sure things could be done. It made it impossible to work between our various offices for a couple of days.

But we have done a number of things to help law enforcement. As Jim Robinson knows, in 1984 we passed the Computer Fraud and Abuse Act to criminalize conduct when carried out by means of unauthorized access to a computer. In 1986, we passed the Electronic Communications Privacy Act, ECPA, which I sponsored, that criminalized tampering with electronic mail systems.

In 1994, the Violent Crime Control and Law Enforcement Act included the computer abuse amendments which I authored to make illegal the intentional transmission of computer viruses. In the 104th Congress, Senators Kyl, Grassley and I worked together to enact the National Information Infrastructure Protection Act.

We have introduced a bill in this Congress with Senator DeWine, the Computer Crime Enforcement Act, to set up a $25 million grant program within the Department of Justice for States to use. All 50 States have tough computer control laws, but they need the training, and this would help greatly. We have seen even in a little State like mine the number of problems we have.

Our computer crime laws need to be kept up to date. We introduced S. 2430 on April 13, the Internet Security Act, that would

do that. The Hatch-Schumer Internet Integrity and Critical Infrastructure Protection Act is scheduled for markup at the committee's next business meeting, and I am very pleased that both Senator Hatch and Senator Schumer are here having this hearing.

I support a number of the provisions in it. In fact, some are virtually identical to sections in my Internet Security Act and my e-rights bill, so I obviously support those. I would raise only the question of some parts of it which would criminalize a variety of minor computer abuses, regardless of whether any significant harm results.

I think we want to look at this. I don't want to be criminalizing an over-curious college sophomore who might check a professor's unattended computer to see what grade he is going to get and accidentally delete a message. I don't think Federal law should go after that. One could argue that under S. 2448, that could constitute a three-year felony. So I think we have to make sure that we do the things we all agree we want to do, not criminalize other aspects. I have mentioned this to the chairman before and to Senator Schumer, and we will continue to work on that.

I don't want to hold up the hearing. I will put the whole statement in the record, Orrin, but I did want to mention those points. There are some parts, as I said, I strongly agree with because they are the same as my bill, but there are other parts that we want to just make sure that we don't overreach on some of these areas of criminalization.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

As we head into the twenty-first century, computer-related crime is one of the greatest challenges facing law enforcement. Many of our critical infrastructures, our government and each of us depend upon the reliability and security of complex computer systems. We need to make sure that both essential government systems and our personal computers are protected from attack. Just recently we were reminded of how vulnerable—and how inter-connected—all of our computer systems are when the "I love you" virus disabled computers all over the world.

*Cybercrime is not a new problem.* We have been aware of the vulnerabilities to terrorist attacks of our computer networks for more than a decade. It became clear to me, when I chaired a series of hearings in 1988 and 1989 by the Subcommittee on Technology and the Law in the Senate Judiciary Committee on the subject of high-tech terrorism and the threat of computer viruses, that merely "hardening" our physical space from potential attack would only prompt committed criminals and terrorists to switch tactics and use new technologies to reach vulnerable softer targets, such as our computer systems and other critical infrastructures. The government has a responsibility to work with those in the private sector to assess those vulnerabilities and defend them. That means making sure our law enforcement agencies have the tools they need, but also that the government does not stand in the way of smart technical solutions to defend our computer systems.

*Encryption helps prevent cybercrime.* That is why, for years, I have advocated and sponsored legislation to relax export controls on encryption technology and encourage the widespread use of strong encryption. The Administration made enormous progress earlier this year when it issued new export regulations on encryption. Of course, encryption technology cannot be the sole source of protection for our critical computer networks and computer-based infrastructure, but we need to make sure the government is encouraging—and not restraining—the use of strong encryption and other technical solutions to protecting our computer systems.

*The private sector must assume primary responsibility for protecting its computer systems.* Targeting cybercrime with up-to-date criminal laws and tougher law enforcement is only part of the solution. While criminal penalties may deter some computer criminals, these laws usually come into play too late, after the crime has been committed and the injury inflicted. We should keep in mind the adage that the best defense is a good offense. Americans and American firms must be encouraged to

take preventive measures to protect their computer information and systems. Just recently, Internet providers and companies such as Yahoo! and Amazon.com Inc., and computer hardware companies such as Cisco Systems Inc., proved successful at stemming denial-of-service attacks within hours thereby limiting losses.

*Prior legislative efforts were designed to deter cybercrime.* Congress has responded again and again to help our law enforcement agencies keep up with the challenges of new crimes being executed over computer networks. In 1984, we passed the Computer Fraud and Abuse Act, and its amendments, to criminalize conduct when carried out by means of unauthorized access to a computer. In 1986, we passed the Electronic Communications Privacy Act (ECPA), which I was proud to sponsor, to criminalize tampering with electronic mail systems and remote data processing systems and to protect the privacy of computer users. In 1994, the Violent Crime Control and Law Enforcement Act included the Computer Abuse Amendments which I authored to make illegal the intentional transmission of computer viruses.

In the 104th Congress, Senators Kyl, Grassley and I worked together to enact the National Information Infrastructure Protection Act to increase protection under federal criminal law for both government and private computers, and to address an emerging problem of computer-age blackmail in which a criminal threatens to harm or shut down a computer system unless their extortion demands are met.

In this Congress, I have introduced a bill with Senator DeWine, the Computer Crime Enforcement Act, S. 1314, to set up a $25 million grant program within the U.S. Department of Justice for states to tap for improved education, training, enforcement and prosecution of computer crimes. All 50 states have now enacted tough computer crime control laws. These state laws establish a firm groundwork for electronic commerce and Internet security. Unfortunately, too many state and local law enforcement agencies are struggling to afford the high cost of training and equipment necessary for effective enforcement of their state computer crime statutes. Our legislation, the Computer Crime Enforcement Act, would help state and local law enforcement join the fight to combat the worsening threats we face from computer crime.

*Computer crime is a problem in Vermont.* I recently released a survey on computer crime in Vermont, my home state. My office surveyed 54 law enforcement agencies in Vermont—43 police departments and 11 State's attorney offices—on their experience investigating and prosecuting computer crimes. The survey found that more than half of these Vermont law enforcement agencies encounter crime, with many police departments and state's attorney offices handling 2 to 5 computer crimes per month.

Despite this documented need, far too many law enforcement agencies in Vermont cannot afford the cost of policing against computer crimes. Indeed, my survey found that 98% of the responding Vermont law enforcement agencies do not have funds dedicated for use in computer crime enforcement.

My survey also found that few law enforcement officers in Vermont are properly trained in investigating computer crimes and analyzing cyber-evidence. According to my survey, 83% of responding law enforcement agencies in Vermont do not employ officers properly trained in computer crime investigative techniques. Moreover, my survey found that 52% of the law enforcement agencies that handle one or more computer crimes per month cited their lack of training as a problem encountered during investigations. Proper training is critical to ensuring success in the fight against computer crime, and the Leahy-DeWine Computer Crime Enforcement Act would help.

*Our computer crime laws need to be kept up-to-date as an important backstop and deterrent.* That is why, on April 13, 2000, I introduced legislation, S. 2430, The Internet Security Act, to help law enforcement investigate and prosecute those who jeopardize the integrity of our computer systems and the Internet, while enhancing protection of online privacy. The Internet Security Act would make it more efficient for law enforcement to use tools that are already available—such as pen registers and trap and trace devices—to track down computer criminals expeditiously. It would ensure that law enforcement can investigate and prosecute hacker attacks even when perpetrators use foreign-based computers to facilitate their crimes. It would allow criminal forfeiture of replicator devices used in the counterfeiting of computer software. It would close a current loophole in our wiretap laws that prevents a law enforcement officer from monitoring an innocent-host computer with the consent of the computer's owner and without a wiretap order to track down the source of denial-of-service attacks. Finally, this legislation will assist state and local police departments in their parallel efforts to combat cybercrime, in recognition of the fact that this fight is not just at the federal level.

The key provisions of the *Internet Security Act* are:

• *Jurisdictional and Definitional Changes to the Computer Fraud and Abuse Act:* The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is the primary federal criminal statute prohibiting computer frauds and hacking. This bill would amend the statute to clarify the appropriate scope of federal jurisdiction.

*First,* the bill adds a broad definition of "loss" to the definitions section. Calculation of loss is important both in determining whether the $5,000 jurisdictional hurdle in the statute is met, and, at sentencing, in calculating the appropriate guideline range and restitution amount.

*Second,* the bill amends the definition of "protected computer," to expressly include qualified computers even when they are physically located outside of the United States. This clarification will preserve the ability of the United States to assist in international hacking cases. A "Sense of Congress" provision specifies that federal jurisdiction is justified by the "interconnected and interdependent nature of computers used in interstate or foreign commerce."

*Finally,* the bill expands the jurisdiction of the United States Secret Service to encompass investigations of all violations of 18 U.S.C. § 1030. Prior to the 1996 amendments to the Computer Fraud and Abuse Act, the Secret Service was authorized to investigate any and all violations of section 1030, pursuant to an agreement between the Secretary of Treasury and the Attorney General. The 1996 amendments, however, concentrated Secret Service jurisdiction on certain specified subsections of section 1030. The current amendment would return full jurisdiction to the Secret Service and would allow the Justice and Treasury Departments to decide on the appropriate work-sharing balance between the two.

• *Elimination of Mandatory Minimum Sentence for Certain Violations of Computer Fraud and Abuse Act:* Currently, a directive to the Sentencing Commission requires that all violations, including misdemeanor violations, of certain provisions of the Computer Fraud and Abuse Act be punished with a term of imprisonment of at least six months. The bill would change this directive to the Sentencing Commission so that no such mandatory minimum would be required.

• *Additional Criminal Forfeiture Provisions:* The bill adds a criminal forfeiture provision to the Computer Fraud and Abuse Act, requiring forfeiture of physical property used in or to facilitate the offense as well as property derived from proceeds of the offense. It also supplements the current forfeiture provision in 18 U.S.C. § 2318, which prohibits trafficking in, among other things, counterfeit computer program documentation and packaging, to require the forfeiture of replicators and other devices used in the production of such counterfeit items.

• *Pen Registers and Trap and Trace Devices:* The bill makes it easier for law enforcement to use these investigative techniques in the area of cybercrime, and institutes corresponding privacy protections. On the law enforcement side, the bill gives nationwide effect to pen register and trap and trace orders obtained by Government attorneys, thus obviating the need to obtain identical orders in multiple federal jurisdictions. It also clarifies that such devices can be used on all electronic communication lines, not just telephone lines. On the privacy side, the bill provides for greater judicial review of applications for pen registers and trap and trace devices and institutes a minimization requirement for the use of such devices. The bill also amends the reporting requirements for applications for such devices by specifying the information to be reported.

• *Denial of Service Investigations:* Currently, a person whose computer is accessed by a hacker as a means for the hacker to reach a third computer cannot simply consent to law enforcement monitoring of his computer. Instead, because this person is not technically a party to the communication, law enforcement needs wiretap authorization under Title III to conduct such monitoring. The bill will close this loophole by explicitly permitting such monitoring without a wiretap if prior consent is obtained from the person whose computer is being hacked through and used to send "harmful interference to a lawfully operating computer system."

• *State and Local Computer Crime Enforcement:* The bill directs the Office of Federal Programs to make grants to assist State and local law enforcement in the investigation and prosecution of computer crime.

*S. 2448, the Hatch-Schumer "Internet Integrity and Critical Infrastructure Protection Act", is scheduled for mark-up at the Committee's next business meeting.* This bill addresses a number of important and complex issues, and I am glad the Chairman decided to hold a hearing before the Committee is asked to vote on it. While I support some of the provisions in the legislation offered by Senators Hatch and Schumer—Indeed, some are virtually identical to sections in my Internet Security Act and in my E-Rights bill—others should give us pause.

For example, section 109 of the Hatch-Schumer bill incorporates provisions from the Leahy-DeWine Computer Crime Enforcement Act, S. 1314, and I certainly support that. I also support sections 301(a) and 303, since they reflect pen register and

wiretap reporting requirements that were in the Leahy-Hatch wiretap reporting bill, S. 1769, which was enacted on May 2, 2000 (P.L. 106–197). I support other sections as well, such as sections 103 (regarding the authority of the U.S. Secret Service) and 107 (regarding forfeiture of replication devices used to counterfeit computer software), which are also part of my Internet Security Act. Finally, I support section 302 of S. 2448, which generally mirrors provisions to provide privacy protection to subscribers of satellite TV services that I proposed over a year ago in my E–RIGHTS bill, S. 854. Despite my support for those provisions, let me explain my concerns with other parts of S. 2448.

*S. 2448 Would Over-Federalize Minor Computer Abuses:* Currently, federal jurisdiction exists for a variety of computer crimes if, and only if, such criminal offenses result in at least $5,000 of aggregate damage or cause another specified injury, such as the impairment of medical treatment, physical injury to a person or a threat to public safety. The Hatch/Schumer bill would criminalize a variety of minor computer abuses, regardless of whether any significant harm results. In addition, for certain computer offenses, the maximum punishment has been doubled.

Specifically, the bill would amend 1030(a)(5)(A) (sending transmissions intending to cause damage), and 1030(a)(5)(B) (intentionally accessing computer and recklessly causing damage) provisions to eliminate the now-existing jurisdictional triggers and to criminalize as 3-year federal felonies all such offenses, whether or not they cause $5,000 loss or other specified injury. In addition, the bill would amend 1030(a)(5)(C) (intentionally accessing computer and causing damage) to eliminate now-existing jurisdictional triggers to criminalize as misdemeanors all such offenses, whether or not they cause $5,000 loss or other specified injury. These minor incidents were not previously punishable under federal law.

These provisions are overkill. Our federal laws do not need to reach each and every minor, inadvertent and harmless hacking offense—after all, each of the 50 states has its own computer crime laws. Rather, our federal laws need to reach those offenses for which federal jurisdiction is appropriate. This can be accomplished, as I have done in the Internet Security Act by simply adding an appropriate definition of "loss" to the statute.

Prior Congresses have declined to over-federalize computer offenses and sensibly determined that all computer abuses warrant federal criminal sanctions. When the computer crime law was first enacted in 1984, the House Judiciary Committee reporting the bill stated: "the Federal jurisdictional threshold is that there must be $5,000 worth of benefit to the defendant or loss to another in order to concentrate Federal resources on the more substantial computer offenses that affect interstate or foreign commerce." (H. Rep., 98–894, at p. 22, July 24, 1984).

Similarly, the Senate Judiciary Committee under the chairmanship of Senator Thurmond, rejected suggestions in 1986 that "the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered." (S. Rep. 99–432, at p. 4, September 3, 1986).

For example, if an overly-curious college sophomore checks a professor's unattended computer to see what grade he is going to get and accidentally deletes a file or a message, current Federal law does not make that conduct a crime. That conduct may be cause for discipline at the college, but not for the FBI to swoop in and investigate. Yet, under S. 2448, this unauthorized access to the professor's computer would constitute a felony violation of 1030(a)(5)(B), punishable by up to 3 year's imprisonment, with mandatory minimum of at least 6 months in jail under U.S.S.G. §2B1.3, or a misdemeanor violation of 1030(a)(5)(C).

Let us look at another example of a teenage hacker, who plays a trick on a friend by modifying the friend's vanity Web page. Under current law, no federal crime has occurred. Yet, under S. 2448, this conduct could constitute a felony violation of 1030(a)(5)(B), punishable by up to 3 years' imprisonment, with mandatory 6-month jail term under U.S.S.G. §2B1.3, or a misdemeanor violation of 1030(a)(5)(C). If the damage to the Web page resulted in more than $5,000 in damage, then the conduct would be punishable by up to 10 years' imprisonment.

Another part of S. 2448 would authorize the Attorney General to provide computer crime evidence to foreign law enforcement authorities under the provisions of a computer crime Mutual Legal Assistant Treaty ("MLAT") and "without regard to whether the conduct investigated violates any Federal computer crime law." This title appears to expand the Justice Department's investigate authority broadly to investigate lawful conduct in the U.S. at the request of foreign governments. Moreover, this title may be construed to force the Justice Department to negotiate MLATs narrowly limited to computer crimes, rather than addressing criminal activity generally, and consequently may require more, not less, work for the Department to obtain constructive assistance from foreign governments in computer crime cases.

I expressed these and other concerns before the Chairman introduced this bill, and would be happy to discuss ways in which we can work together on these important issues.

*Legislation must be balanced to protect our privacy and other constitutional rights.* This hearing has two subjects—both Internet security and privacy. This is appropriate since secure systems that keep out unauthorized snoops are integral to maintaining the privacy of our electronic mail messages and the information we store on our PC's hard drive or on a remote server. I am a strong proponent of the Internet and a defender of our constitutional rights to speak freely and to keep private our confidential affairs from either private sector snoops or unreasonable government searchers. We must make sure that our legislative efforts are precisely targeted on stopping destructive acts and that we avoid scatter shot proposals that would threaten, rather than foster, electronic commerce and sacrifice, rather than promote, our constitutional rights.

*Process is important.* Technology has ushered in a new age filled with unlimited potential for commerce and communications. But the Internet age has also ushered in a new challenges for federal, state, and local law enforcement officials. Congress, the Administration and the private sector need to work together to meet these new challenges while preserving the benefits of our new era. We should not be rushing forward with legislation without engaging in discussions with the Administration and industry to ensure the legislation addresses problems constructively without inadvertently creating other problems.

The CHAIRMAN. Well, thank you, Senator Leahy. We look forward to working very closely with you. You and I have worked on almost every intellectual property bill that has come through the Congress. And we can't do it without you, so we just appreciate any suggestions you have.

We have already heard from Mr. Vatis. We are going to turn to Mr. Robinson. We are certainly happy to have you with us here today, and also you, Ms. Stansell-Gamm.

## STATEMENT OF JAMES K. ROBINSON

Mr. ROBINSON. Thank you, Mr. Chairman, Senator Leahy, Senator Schumer. I want to thank you for this opportunity to testify on the topic of cyber crime and S. 2448, the Internet Integrity and Critical Infrastructure Act, sponsored by the chairman and Senator Schumer.

The issue, as you have all indicated in your statements, before the committee today is one of singular importance in our technologically advancing world. I want to thank you personally, Mr. Chairman, and Senator Leahy, for your leadership and your help to law enforcement not only on this issue, but on many matters dealing with public safety over the years.

Chairman Hatch, we have been pleased to work with you on a number of initiatives to help law enforcement, and we sincerely appreciate your efforts to address the current challenges we face in cyberspace by introducing S. 2448, along with Senator Schumer, and for holding this hearing today.

Senator Leahy has also been a pivotal person, as we know, in the development of many of the most prominent statutes utilized today against online criminals, such as the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act. And your efforts, Senator Leahy, to protect the online public have continued recently, as you have indicated, with the introduction of S. 2430, the Internet Security Act of 2000.

The Department appreciates the continued dedication of this committee and the leadership of this committee on these very important issues, and it is our sincere hope that we will be able to

work together in the remaining days of this Congress to help ensure the safety of all Americans who use the Internet.

As was noted by the chairman, over the past decade the use of computers and the Internet has grown exponentially, and individuals have increasingly come to depend on the use of this very important technological tool in their daily lives. The Internet has resulted in new and exciting ways for people to communicate, to transfer information, engage in commerce, and expand their educational opportunities.

Yet, as has been noted, as people have increasingly used computers for lawful purposes, so too have criminals increasingly exploited computers to commit crimes and to harm the safety, security, and privacy of all American citizens in many instances.

Just in the past few months, for example, legitimate e-commerce has been the target of malicious computer hackers in the form of denial of service attacks that have been mentioned. These unlawful attacks involve the intrusion into an unknown number of computers which are used to use launch attacks on target computers. In these cases, the number of victims can be substantial, as can the collective costs and loss and the cost to respond to these attacks.

These fast-moving viruses that we have seen recently are also a matter of major concern. As Mr. Vatis indicates, while these denial of service attacks and the recent viruses have received a great deal of attention and are certainly a cause of concern by all of us, they are but one facet of the criminal activity that occurs online today.

Criminals use computers to send child pornography to each other using anonymous encrypted communications. Hackers illegally break into financial computers and steal sensitive personal information of private consumers, such as names, addresses, Social Security numbers, and credit card information. Criminals use the Internet's inexpensive and easy means of communication to commit large-scale frauds on victims all over the globe.

Simply put, criminals are exploiting the Internet and victimizing people worldwide every day.

The growing threat of illicit conduct online was made clear in the findings and conclusions recently released in the report of the President's Working Group on Unlawful Conduct on the Internet which I have a copy of here, entitled "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." The report highlights in detail the significant challenges facing law enforcement in cyberspace. I would encourage any interested persons to consult the Computer Crime and Intellectual Property Section's Web site for this information, as well as other information. It is www.cybercrime.gov.

The migration of criminal activity to cyberspace has accelerated and continues to accelerate with each passing day, and the threat to public safety is becoming increasingly significant. As a consequence, the work of this committee in this important area is essential to the protection of all Americans.

It is fair to say, as this committee has recognized, that the laws defining computer offenses and the legal tools needed to investigate criminals using the Internet have lagged behind the technological and social changes which have occurred so rapidly, leaving many of these tools and law out of date and in some instances ineffective.

In short, law enforcement today does not have the tools needed to fully protect the Internet-using public from online criminal activity. It is not a coincidence that this is the fourth time since February of this year that the Department of Justice has provided testimony on this issue to Congress.

The safety of the Internet-using public is and will remain a priority for the Justice Department. I would note, for example, that earlier this year the Attorney General and the FBI Director participated in the creation of the Internet Fraud Complaint Center, which gives consumers the ability to go online and file complaints with the Center. This is but one aspect of the approach taken by the FBI and the Department to making cyberspace a safe place for everyone.

Because of the gravity of this issue and the need to respond quickly, I am pleased to offer our preliminary views in my testimony that has been filed with the committee on S. 2448, and I want to say at the outset that the proposed legislation, I think, appropriately focuses on several very important public safety goals. I will just mention this briefly, in the interest of time.

First, I think the legislation improves the ability of Federal investigators and prosecutors to bring online criminals to justice by removing the $5,000 damage threshold for Federal jurisdiction. The Department has encountered difficulties in this area of getting over this threshold, and we think it is particularly important to address that and we commend the committee and the sponsors for doing that.

Second, I think the bill greatly enhances the deterrent effect of the Computer Fraud and Abuse Act, the primary statute used to prosecute computer hackers, by raising the maximum penalties for various categories of violations, such as those that occurred in the recent denial of service attacks which have been discussed earlier. Given the scope and severity of the damage to protected computers that have occurred recently, the current five-year maximum, we think, does not adequately take into account the seriousness of these crimes.

The statute also provides for increased punishment for computer criminals that use minors to help in the commission of crime. And the Department shares your concern about adults exploiting children to aid in the furtherance of their own criminal activities, and this deserves special condemnation. We are concerned, however, that the provision may be only applicable to adults who use juveniles and not to—we are concerned about having that provision apply to juvenile co-conspirators, something I am sure the committee will look at carefully.

We think that the efforts to address greater deterrence to would-be juvenile hackers is an appropriate consideration, something that we think is fully worthy of being addressed. And to address this important problem, the bill provides that juvenile adjudications for the Computer Fraud and Abuse Act count as prior convictions as other similar provisions. We support your efforts to address these issues and to assist law enforcement in combatting crime effectively and promoting public safety online.

In the interest of time, I would just mention two other quick matters of interest to us. I think one is that the Department be-

lieves it is critical to modernize the outdated trap and trace and pen register statutes to eliminate unworkable and technologically specific terminology, and to provide courts with the ability to issue orders that under the statute have a nationwide effect. It is a major deterrent in this fast-moving area where you have to track these communications to have go to through so many chains, and I think that is a very important development. Indeed, S. 2092, introduced by Senators Schumer and Kyl, addresses these issues and we think that is an important development.

Another thing I want to mention briefly is the Department continues to be concerned about technology-specific legislation and statutes. Things are moving so quickly in this world that our concern is that the proposed section 302 of S. 2448 regarding satellite television services would, as introduced, create many of the same problems we have seen in other instances when technology-specific legislation is adopted.

At present, existing statutes that are written in technology-specific terms have resulted, we think, in unintended conflict with other Federal laws, such as ECPA. This has led to litigation that has slowed down unnecessarily, we think, criminal investigations. We believe that ECPA does apply to all communication providers without regard to specific technology used to provide the services. And for these reasons, we would recommend that section 302 be removed.

Obviously, we have focused on some of the more significant matters in our filed testimony, not intended to be all-inclusive. The Department has provided our full written statement. We look forward to working with the committee in these and other efforts to address this very important problem, and we are happy to answer your questions.

I am particularly happy to be here with Marty Stansell-Gamm, the Chief of our Computer Crimes and Intellectual Property Section in the Criminal Division. This is an outstanding group of prosecutors who are working at the cutting edge, with your help and providing them the tools to do so. And I think the country can be proud of the efforts of these very able prosecutors and the people we have in all the U.S. Attorneys' offices around the country working to assist all of us in dealing with this important problem.

So I thank you very much for your interest and look forward to trying to provide answers to your questions.

[The prepared statement of Mr. Robinson follows:]

PREPARED STATEMENT OF JAMES K. ROBINSON

Mr. Chairman, Senator Leahy and Members of the Committee, I thank you for this opportunity to testify on the topic of cybercrime and S.2248, The Internet Integrity and Critical Infrastructure Act sponsored by Chairman Hatch and Senator Schumer. The issue before this Committee today is one of singular importance and I commend the Committee for holding this hearing today. I also want to thank you personally Mr. Chairman and Senator Leahy for your leadership, not just on this issue, but on many matters dealing with public safety over the years.

Chairman Hatch we have been pleased to work with you on a number of initiatives to help law enforcement and we sincerely appreciate your efforts to address the current challenges facing us in cyberspace by introducing S. 2448, along with Senator Schumer, and for holding this hearing today. Senator Leahy, you have been a pivotal person in the development of many of the most prominent statutes utilized today against online criminals, such as the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act. Your efforts to protect the online public

have continued recently with the introduction of S. 2430, The Internet Security Act of 2000. The Department of Justice appreciates the continued dedication and leadership of you both to these important issues. It is my sincere hope that we will all be able to work together in the remaining days of this Congress to help ensure the safety of all Americans who use the Internet.

THE INTERNET AND PUBLIC SAFETY

Over the last decade, use of computers and the Internet has grown exponentially, and individuals have increasingly come to depend on this use in their daily lives. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. There is no question that the Internet has changed the way we live today. Yet, as people have increasingly used computers for lawful purposes, so too have criminals increasingly exploited computers to commit crimes and to harm the safety, security, and privacy of others.

In just the past few months for example, legitimate e-commerce has been the target of malicious computer hackers in the form of "denial of service attacks." These unlawful attacks involve the intrusion into an unknown number of computers, which are in turn used to launch attacks on several, target computers, such as Yahoo, eBay, CNN and ZDNET. In these cases, the number of victims can be substantial, as can the collective loss and cost to respond to these attacks. We have also seen the emergence of fast-moving viruses that have caused damages to computer systems around the world and have disrupted the computer systems of consumers, businesses, and governments.

In April 1999, the Melissa virus was released. Through the cooperative efforts of state and federal law enforcement, as well as the contributions of antiviral companies and Internet service providers, the perpetrator of the virus was found within a few days of the virus' dissemination. He pled guilty in December, admitting that his actions caused over $80 million in damages.

A few weeks ago, the "I Love You" virus began infecting systems around the world. While there is not yet any official assessment of the damages caused by this virus, antiviral companies have estimated that the damages are in the billions. As with the Melissa virus, law enforcement agencies on all levels have been cooperating with the private sector to determine who released this virus. The FBI is now working closely with the National Bureau of Investigation of the Philippines to pursue leads in that country. While I cannot comment directly on that investigation, I will say that the FBI and the Department of Justice will continue to provide whatever technical, investigative, or prosecutorial assistance is needed by the Philippine government.

Frighteningly, the "I Love You" virus was followed almost immediately by copycat variants. At last count, there were almost 30 of these variants that had been identified. They were followed last Thursday by the New Love virus, a virus that self-replicated, mutated in name and size, and destroyed the computer systems affected by it. The FBI, again working with the private sector, is investigating.

The new crop of viruses are becoming more sophisticated and difficult to detect. If we are going to control this epidemic of viruses and denial of service attacks, U.S. law enforcement must continue to work with the private sector and with law enforcement in other countries. As all these cases demonstrate, computer crime is a global problem. In this regard, we are making important progress. Last week, I returned from a meeting in Paris at which the government and industry of the G8 nations, along with representatives of other nations and groups, sat down to discuss how we can work together to identify the source of criminal behavior on the Internet, as well as tracing those responsible for committing crime over the Internet. We are also involved in similar efforts with the Council of Europe. Efforts are underway, which are nearing completion, to develop a cybercrime convention that will create minimum standards for defining crimes committed over the computer networks. The convention will also establish minimum standards for international cooperation and domestic law enforcement powers. The draft convention also would further expand the 24/7 point of contact network that was begun by the G8. This network of experienced law enforcement officials capable of dealing with computer crime has been steadily expanding beyond its original eight members, and we are working to further develop the network so that we are better prepared to address crimes committed using computer networks wherever and whenever they occur.

Fostering better international understanding and response to computer crimes has been a priority for over a decade and we are making significant progress. We will continue to build on the successes of the past and capitalize on world-wide at-

tention brought about by the "I Love You" virus to continue working with nations across the globe on this vital issue.

While the denial of service attacks and the recent viruses have received a great deal of attention and are cause for concern, they are but one facet of the criminal activity that occurs online today. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers illegally break into financial computers and steal sensitive, personal information of private consumers, such as name, address, social security number and credit card information; criminals use the Internet's inexpensive and easy means of communication to commit large-scale fraud on victims all over the globe. Simply put, criminals are exploiting the Internet and victimizing people, worldwide, everyday.

It is important to note, Mr. Chairman, that when law enforcement successfully investigates, apprehends, and prosecutes a criminal who has stolen a citizen's personal information from a computer system, law enforcement is undeniably working, not just to apprehend the offender, but to protect privacy and deter further privacy violations at the hands of criminals. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

RESPONDING TO THE CHALLENGE OF UNLAWFUL CONDUCT ON THE INTERNET

The growing threat of illicit conduct online was made clear in the findings and conclusions reached in the recently released report of the President's Working Group on Unlawful Conduct on the Internet, entitled "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet." This extensive report highlights in detail the significant challenges facing law enforcement in cyberspace. As the report states, the needs and challenges confronting law enforcement, "are neither trivial nor theoretical." The Report outlines a three-pronged approach for responding to unlawful activity on the Internet:

1. Conduct on the Internet should be treated in the same manner as similar conduct offline, in a technology neutral manner.

2. The needs and challenges of law enforcement posed by the Internet—including the need for resources, up-to-date investigative tools and enhanced multijurisdictional cooperaton—are significant.

3. Finally, continued support for private sector leadership in developing tools and methods to help Internet users to prevent and minimize the risks of unlawful conduct online.

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report an be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at *www.cybercrime.gov*. That website also contains a great deal of other information relating to cybercrime and to the laws protecting intellectual property.

The migration of criminality to cyberspace accelerates with each passing day and the threat to public safety is becoming increasingly significant. As Deputy Attorney General Eric Holder told a joint hearing of House and Senate Judiciary Subcommittees in February, this nation's vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

However, Mr. Chairman, the laws defining computer offenses—and the legal tools needed to investigate criminals using the Internet—have lagged behind technological and social changes, leaving them out of date and, in some instances, ineffective. In short, law enforcement today does not have the tools we need to fully protect the Internet-using public from criminal activity online.

We must confront this problem on two fronts simultaneously. First, we must make certain that the substantive laws defining which conduct is criminal, such as the Computer Fraud and Abuse Act (Title 18 section 1030), are adequately refined and updated. Second, we must look critically at the tools law enforcement uses to investigate and prosecute computer crimes—such as the Electronic Communications Privacy Act and the pen register and trap and trace statutes—to ensure that they are cast in terms that fully account for the rapid advances in technology. Failure to do both will render our efforts meaningless. If we have the appropriate substantive laws, but no means to effectuate them, we will be stymied in our pursuit of online criminals. Conversely, if the conduct in question is not covered by the criminal law, the ability to gather evidence is of no value in protecting the safety and privacy of people who use the Internet. It is not a coincidence, Mr. Chairman, that today marks the fourth time, since February of this year, that the Department of Justice has provided testimony on this issue to Congress. This issue—the safety of the Internet-using public—is and will remain a priority of the Justice Depart-

ment. I would note, for example, that earlier this month the Attorney General and the Director of the FBI participated in the creation of the Internet Fraud Complaint Center, which gives consumers the ability to go online and file complaints with the Center. This is but one aspect of the approach we are taking to make cyberspace safe for everyone.

DEPARTMENT OF JUSTICE VIEWS ON S. 2448

At this point, I am pleased to offer the preliminary views of the Department of Justice on S. 2448, "The Internet Integrity and Critical Infrastructure Protection Act," that is the subject of today's hearing.

At the outset, let me say that the proposed legislation appropriately focuses on several very important public safety goals. As I mentioned earlier, the ability to fully protect public safety online requires that the substantive laws utilized to define criminal activity be fine-turned. The proposed legislation, S. 2448, offers a number of provisions that address the substantive laws.

*A. Refining the substantive law for the Information Age*

First, the legislation addresses the ability of federal investigators and prosecutors to bring online criminals to justice by removing the $5,000 "damage" threshold for federal jurisdiction. The Department has encountered numerous instances in which computer intruders have gained unauthorized access to computers used in the provisions of "critical infrastructure" systems and services, which include, for example, computers that run 9–1–1 emergency services.

Yet, in several investigations, proof of damage in excess of $5,000—the amount presently required to allow federal investigation and prosecution—has not been readily available. Given the risks posed by the initial act of gaining unauthorized access to these vital computers, federal jurisdiction should not be restricted to those instances in which damage of $5,000 or more can be readily demonstrated, under the current definition of "damage". S. 2448 acknowledges and solves this problem by making federal jurisdiction clearly attach at the outset of an unauthorized intrusion into interstate systems, rather than requiring investigators to wait for estimates of damage to confer jurisdiction. While the Justice Department has some concern about treating the newly covered crimes as felonies in every instance, we strongly support this idea, and would like to work with Congress to best determine the appropriate classification of offenses below the $5,000 damage amount. It is, however, vital to our ability to respond to criminal activity that the jurisdictional threshold be removed.

Second, the bill enhances the deterrent effect of the Computer Fraud and Abuse Act—the primary statute used to prosecute computer hackers—by raising the maximum penalties for various categories of violations, such as those that occurred in the recent denial of service attacks discussed earlier. At present, the statutory maximum penalty for these violations is five years. Given the scope and severity of the damage to protected computers that hackers have been doing recently, the current five year maximum does not adequately take into account the seriousness of their crimes.

For example, as I mentioned earlier, David Smith recently pled guilty to violating Title 18, subsection 1030(a)(5)(A), for releasing the "Melissa" virus that caused massive damage to thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of damage (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the actual amount of damage may have been as much as ten times that amount. Depending on the circumstances of the offense, the amount of loss and the criminal history of the offender, the Sentencing Guidelines may call for a sentence of greater than five years. However, such a sentence cannot be imposed at this time. We support the goal of raising penalties for violations of the Computer Fraud and Abuse Act and will work with the Committee to determine the appropriate increase.

S. 2448 also provides for increased punishment for computer criminals that "use" minors to help in the commission of the crime. The Department shares your concern that adults that exploit children to aid in the furtherance of their own criminal activity deserve special condemnation. We might explore whether this provision be applied to all of 18 U.S.C. 1030 and not just subsection (a)(5). The Department points out, however, that the provision only be applicable to adults who use juveniles and not to juvenile co-conspirators, and we look forward to working with you to ensure the provision is tailored appropriately.

Third, S. 2448 takes important steps to provide greater deterrence to would-be juvenile hackers. We are increasingly encountering juveniles committing crimes and creating risks to the public via the Internet. For example, a juvenile was recently charged with the recent "denial of service" attack on CNN. This juvenile, known as

"Mafiaboy," is currently being prosecuted in Canada. We have also seen juvenile hackers penetrate numerous sensitive computers, including computers run by the Defense Department, even as military operations were being planned. In addition, in March of 1998, a juvenile hacker interfered with a computer that provided telecommunications of a town in central Massachusetts, including the regional airport. This action cut off telephone service to the airport's control tower, fire department, and security services.

To address this important problem, the bill provides that juvenile adjudications for violations of the Computer Fraud and Abuse Act count as prior convictions if such juveniles continue to violate section 1030 as adults. Thus, any juvenile who is arrested and adjudicated delinquent for such a crime would face a stiffer penalty if he or she does not reform. The bill also modifies federal law to allow the federal government to investigate and prosecute juveniles who commit certain serious computer offenses. As S. 2448 recognizes, when an individual attacks a federal computer, or when a hacker uses interstate communications or the Internet to compromise the health, safety, or security of the public, it clearly raises substantial federal interest and warrants federal jurisdiction.

Mr. Chairman, we support your efforts to address these issues and assist law enforcement to combat crime effectively and promote public safety online. As mentioned earlier, however, revision of the substantive law is but one needed part of the response to cybercrime. The balance of my testimony, and the views of the Department of Justice on S. 2448, will focus on the second prong—making certain that law enforcement has the tools necessary to investigate and build cases against online criminals.

*B. Updating the tools needed to protect public safety online*

Section 301 of the proposed legislation attempts to solve several important problems relating to the use of pen registers and trap and trace devices in the investigation of computer crime. The Justice Department is concerned, however, that as introduced, this section of the bill does not address several problems in the existing statute that have been caused by changes in telecommunications technology and the telecommunications industry. First, the language of the existing law is obsolete. The definition of "pen register," for example, refers to a "device" that is "attached" to a telephone "line." Telephone companies, however, no longer accomplish these functions using physical hardware attached to an actual telephone line. Moreover, the existing statute refers specifically to telephone "numbers," a concept made out of date by the need to trace communications over the Internet that use other means to identify users' accounts. The Department strongly recommends that these provisions be amended to clarify that pen/trap orders apply equally to the tracing of communications in the computer network context. Indeed, S.2092, introduced by Senators Schumer and Kyl, would amend the statute in these important ways.

In addition to amending the language of the statute to reflect the technological changes that have and will continue to occur, the Justice Department also recommends that the statute be amended to ensure that federal courts have the authority to order all telecommunications carriers providing service in the United States—whether within a particular judicial jurisdiction or not—to provide law enforcement authorities the information needed to trace both voice and electronic communications to their source. The deregulation of the telecommunications industry has created unprecedented hurdles in tracing multi-provider communications to their ultimate source and destination. Many different companies, located in a variety of judicial districts, may handle a single communication as it crosses the country. Under the existing statute, however, a court can only order the installation of a pen/trap device within the jurisdiction of that court. As a result, investigators often have to apply for multiple court orders in multiple jurisdictions in order to trace a single communication, causing a needless waste of resources and delaying and impeding important investigations. Given that time is of the essence in the vast majority of computer hacking cases, this delay may be fatal to the investigation. S. 2092 address this problem as well.

Section 302 of the proposed legislation regulates the release of personally identifiable information by providers of satellite television services. Although the protection of the privacy of satellite subscribers' information is a laudable goal, the manner in which this provision seeks to address this issue creates serious concerns. This provision is drafted in "technology specific" terms. The Justice Department has consistently argued, and does so today, that in order to be effective, statutes must remain technology neutral. By creating a standard exclusively for one form of technology—in this case, satellite television service—the provision restricts the activities of certain companies and individuals based on an arbitrary criterion. If a company

chooses to provide its television programming over cable lines or over the Internet, it would not be bound by these restrictions.

The law should not treat companies differently based on the various ways in which they provide the identical service. further, the Justice Department is concerned about he scope of services—beyond simply providing television service—that would be covered by this provision, thus compounding the disparate treatment noted above. Given the fact that the old distinctions between communications providers and their respective services are rapidly falling away—with each industry crossing over into other areas and offering multiple communications services—technology specific statutes simply become unworkable. We believe that ECPA governs all communication providers without regard to specific technology used to provide the services.

Another portion of S. 2448 which raises significant concerns for the Department of Justice is Title V, regarding International Computer Crime Enforcement. International cooperation in computer crime cases—as highlighted in recent weeks—is extremely important, and strengthening international cooperation mechanisms is a high priority for the Department. As I noted earlier, we are making significant progress in this area and any new proposals have to be fashioned extremely carefully so as not to undermine the valuable avenues of cooperation already in place. The Department is concerned that Title V would not significantly promote international cooperation on computer crime investigations, and it has the potential to damage existing agreements and legal authorities. The Department, therefore, opposes inclusion of this provision in the bill.

Before concluding my testimony, let me make some brief remarks on two issues that have principally been handled by parts of the Administration other than the Department of Justice. Concerning the anti-slamming provision in S. 2448, the Administration agrees that the use of deceptive identification information in connection with unsolicited commercial email raises serious concerns. While the Administration has not endorsed any currently proposed approach to this problem, we support continued examination of this issue and note that comprehensive antispamming legislation has been proposed in and is being considered by both the House and the Senate at this time.

Concerning the online collection and dissemination of personally identifiable information on Internet, I draw your attention to a statement on that subject earlier this week by Secretary of Commerce Daley. Secretary Daley expressed the hope that we will continue to see improvement in the quantity and quality of online privacy policies. He stated that, "if we do not see such progress, then we may eventually need to consider whether legislation would provide companies with the right incentives to have good policies and participate in an effective self-regulatory program." Secretary Daley added that any such legislation, if it becomes necessary "should recognize and provide incentives for self-regulation, such as by granting participants in effective self-regulatory programs a "safe harbor" from regulation. Such incentives are not currently included in S. 2448.

## CONCLUSION

Mr. Chairman, my testimony today is necessarily focused upon the more significant portions of the proposed legislation and is not intended to be all inclusive. It is my sincere hope that through this and other hearings that have been held, those of us who are concerned about public safety and want to see the Internet continue to flourish and thrive, can come together and forge responses to the problems that I have outlined here today. I again want to commend this Committee for its continued leadership on the issues of technology and public safety and pledge to you today that the Department of Justice stands ready to work with all concerned to make the Internet safe for all Americans.

If we fail in our responsibility to respond to criminal conduct online, we will, in effect render cyberspace a safe haven for criminals. If we do not make the Internet safe, people's confidence in using the Internet and e-commerce will decline, parents will no longer let their children use the Internet for the wonderful learning tool that it is, and people worlds apart will no longer use the Internet to communicate and the flow of information will slow. By failing to ensure the public's safety online, we are effectively endangering the very benefits born of the Information Age. The Internet Integrity and Critical Infrastructure Protection Act is a positive step in avoiding that unfortunate and unnecessary result and we look forward to working with the Committee and the Congress on this matter in the weeks ahead.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.

The CHAIRMAN. Well, thank you, Mr. Robinson.

We have two back-to-back votes. I would like to finish this panel, so I am willing to submit my questions.

The CHAIRMAN. Let me turn to the ranking member. Do you have anything you want to——

Senator Leahy. I will submit mine, also, Mr. Chairman.

[The questions of Senators Hatch and Leahy can be found in the appendix.]

Senator LEAHY. I also want to submit for the record an article from the Washington Post today about security lapses at airports, the Pentagon, and the FBI. It is not just cyberspace that is the problem. We saw it happen at the FBI where people saying that they were law enforcement and had briefcases with weapons in them just got waved through. Of course, they were not law enforcement. It was just a test of security.

I would put that in the record.

[The article referred to follows:]

# Probe Finds Security Lapses At Airports, Pentagon, FBI

By Susan Schmidt
Washington Post Staff Writer
Thursday , May 25, 2000 ; A02

Investigators masquerading as armed law enforcement officers carried unsearched briefcases past security guards at Reagan National Airport and secure government buildings--including the Pentagon, the FBI and the State Department--penetrating into or near Cabinet secretaries' suites in almost every attempt, according to new findings by the General Accounting Office.

Startling security weaknesses were discovered at two airports and all 19 of the federal agencies visited by special GAO investigators, who used counterfeit identification and phony law enforcement badges they obtained on the Internet.

The results of the investigation were shared with the agencies at a closed-door briefing on Capitol Hill on Tuesday morning. The FBI and some other agencies immediately tightened security.

The lapses suggest how vulnerable federal facilities remain to potential acts of terrorism or espionage, even though many buildings are now equipped with metal detectors and protected by concrete barricades.

Late last year, a listening device transmitting to a Russian foreign intelligence officer was discovered in a seventh-floor conference room at the State Department. U.S. officials believe someone penetrated State Department security not only to install the device but to regularly maintain it.

The GAO reported that at every federal building tested, undercover investigators posing as plainclothes officers of the FBI, Drug Enforcement Administration and New York City Police Department were waved around metal detectors when they announced that they were carrying weapons.

In some cases, they were able to roam freely through the buildings and were easily able to locate the agency head's office from room numbers listed in publicly available federal directories. The CIA was the only place where they were unable to reach the office of the department or agency head.

The phony officers--who did not actually carry guns--were able to drive a rental van into the interior courtyard of Justice Department headquarters and simply walk away from it.

"This is a shocking report revealing a dangerous vulnerability plaguing thousands of people who work in our public buildings," House Judiciary Committee Chairman Henry J. Hyde (R-Ill.) said in a statement. A Judiciary subcommittee concerned about the easy availability of stolen and counterfeit law enforcement credentials commissioned the GAO investigation.

At the two airports tested--Reagan National and Orlando International--the fake law enforcement officers were not searched and were given permits to carry weapons aboard airplanes.

GAO Special Investigations official Bob Hast, in a memo prepared for Tuesday's briefing, said the undercover team that penetrated secure locations "could have introduced weapons, explosives, chemical/biological agents, listening devices or other hazardous material."

Said FBI spokesman John Collingwood: "This was a little bit of a wake-up call for every agency put to the test." He added that security measures were changed within an hour after the conclusion of Tuesday's GAO briefing.

"Because people got into the building using false police ID, we changed our internal procedures. All non-FBI law enforcement officers have to surrender their weapons when they come in the building," Collingwood said. New efforts are being made to verify visitors' identification, he said, and visitors will not be able to enter the building unless they have appointments with people authorized to let them in.

Crime subcommittee Chairman Bill McCollum (R-Fla.) said the GAO findings point to a "system-wide breakdown," because investigators were able to penetrate every location they tested. He said the fake badges and IDs were not

intended to be perfect counterfeits. The investigators created the IDs by using computer graphics and bought badges over the Internet and at police supply stores.

McCollum faulted "certain customs and courtesies being extended within the law enforcement community." His subcommittee plans a hearing on the security problem today.

The GAO team not only brought an unsearched vehicle into the Justice Department's courtyard, but made its way up to the area of Attorney General Janet Reno's office suite, though she was not there at the time. The undercover agents were asked to leave by members of the attorney general's staff.

The availability of counterfeit IDs noted by the GAO "has raised some concerns--it's caused us to review and amend our security procedures," Justice Department spokeswoman Gretchen Michael said yesterday. She declined to discuss specific changes.

At the Pentagon, a spokesman said a review of security was recently initiated. "It's been a professional courtesy to allow other law enforcement in without going through the metal detector," he said. In addition to the fake IDs, members of the GAO team were allowed into the Pentagon because some security people recognized them as law enforcement officials, he said.

Those courtesies may be abolished and escorts may be required, the spokesman said.

Mr. ROBINSON. I might just say that I was surprised to see that, since I have so much difficulty getting into the FBI building to meet with senior FBI officials, as anybody who has tried to do that has.

Senator LEAHY. I find the same thing. I find that sometimes both at the State Department and elsewhere on matters when I am handling oversight on major issues for them and their requests come down and I just can't get anywhere. I should just tell them I am carrying my .44 magnum and I am the deputy sheriff of Chittenden County, VT, and I will get waved right in. If I say I am a U.S. Senator, it is a lot more difficult.

The CHAIRMAN. We have a lot of questions that range from what is the Department doing to ensure the privacy rights of online users so that they are not compromised during the effort to patrol and investigate online criminal activity, to the viruses that we have, and isn't our greater threat hostile foreign nations or international or domestic terrorists. How do we combat all of that? We were going to go into PDD–63 and all the issues involved there. So we will submit these because I don't want to have to hold you.

I apologize to the next panel because you are just going to have to wait until we can get back. But if you could answer these questions in as much detail as you can and also give us as succinctly as you can what you think he changes ought to be in this bill—naturally, we file these bills and then we want criticism; we want to know how we can perfect them and make them better.

This is a real important bill and it should give you the tools that law enforcement needs to make sure that we don't have processes that really will hurt our people, our country, and our allies as we continue through this next century.

So with that, I think we will just release you and let you go, and then we will be back as soon as we can get through that second vote and have the second panel. Thanks so much.

[The committee stood in recess from 10:55 a.m. to 11:35 a.m.]

The CHAIRMAN. Well, I apologize. I get grabbed six ways from Friday every time I get near the floor, so there is nothing I can do about that.

Let me call our second panel of witnesses. Our first witness is Bruce Heiman, who is the Executive Director of Americans for Computer Privacy, a coalition of companies, associations, interest groups, and individuals that focuses on issues at the intersection of electronic information, privacy, law enforcement, and national security.

The next witness is Richard Pethia, who is the Director of the CERT Centers, which are a part of the Software Engineering Institute at Carnegie Mellon University, in Pittsburgh, Pennsylvania.

Our third witness is Jeff Richards, Executive Director of the Internet Alliance, located here in Washington D.C.

Our final witness is James X. Dempsey, Senior Staff Counsel with the Center for Democracy and Technology, also located here in Washington, DC.

So I would like to welcome each of you here this morning. We look forward to taking your testimony. We will turn to you first, Mr. Heiman.

And we are happy to have Senator Feinstein here as well.

**PANEL CONSISTING OF BRUCE J. HEIMAN, EXECUTIVE DIRECTOR, AMERICANS FOR COMPUTER PRIVACY, WASHINGTON, DC; RICHARD PETHIA, DIRECTOR, CERT CENTERS, SOFTWARE ENGINEERING INSTITUTE, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA; JEFF B. RICHARDS, EXECUTIVE DIRECTOR, INTERNET ALLIANCE, WASHINGTON, DC; AND JAMES X. DEMPSEY, SENIOR STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC**

**STATEMENT OF BRUCE J. HEINMAN**

Mr. HEIMAN. Thank you, Mr. Chairman, Senator Feinstein. During the last 2 years, Americans for Computer Privacy, ACP, led the private sector effort to encourage the widespread use of American encryption products. With strong congressional support, including many on this committee, we succeeded in persuading the administration to change its policy and relax export controls. That is important because greater use of encryption will help prevent cyber crime and help protect our national security.

But we all know that more needs to be done to protect our critical information infrastructure. ACP takes extremely seriously the need for increased cyber security throughout those sectors of our economy that are so reliant on information systems. We really think there is only one way to get this right. ACP strongly believes that a voluntary, cooperative partnership between government and industry is the only approach that can succeed in protecting critical information infrastructure.

So what should the private sector do? First, companies need to keep improving information security, just as they have been doing for years. It is the private sector that owns and operates the networks, systems, products, and services that make up the information infrastructure. It also is the private sector that possesses the knowledge and expertise necessary to protect it. Unfortunately, there is no single silver bullet for the problem of information security. Rather, it is a process of continual improvement.

Second, we all have to practice good security hygiene and teach others to do so. We have made some progress. According to a recent Pew poll reported in the Washington Post, only about a quarter of those who received the Love Bug e-mail and attachment actually opened it. That is real improvement. You wouldn't let anybody into your house and you shouldn't let just anybody into your computer.

Third, industry does need to share information among itself and with the Government about threats and vulnerabilities, as well as best practices. In this regard, ACP has met with representatives of the National Security Council, the FBI, and the Department of Commerce. Furthermore, several of ACP's members will be serving on the President's National Infrastructure Assurance Council, a CEO-level group that is being formed to advise the President and Cabinet. Many of ACP's members are also active participants in the Partnership for Critical Infrastructure Security, a cross-sector, cross-industry effort led out of the Department of Commerce.

Of course, the Government also has an essential role to play. There are five things the Government should do. First, it is important for the Government to share information quickly with the private sector. This includes alerts of particular threats.

Second, the Government must lead by example. The Government needs to do a better job of protecting its own computer systems.

Third, the Government needs to increase training of law enforcement personnel, including those at the State and local levels. ACP strongly supports funding for this purpose.

Fourth, the Government needs to strengthen its technological capabilities. ACP supports funding so that law enforcement has the same state-of-the-art hardware and software possessed by criminal hackers.

Fifth, we support the idea of new cyber security scholarships and the creation of a new cyber corps of those with specialized education in cyber security.

I want to conclude with an important point. ACP strongly believes that the Government must proceed cautiously and should not rush to pass new legislation. There is little doubt that true cyber crime today is already illegal under our existing laws and can be prosecuted. Moreover, the private sector will continue to cooperate with and assist law enforcement in investigating and prosecuting cyber criminals, just as it has done in the past.

We are concerned about the possibility of overreaction to recent denial of service attacks and Internet viruses. It is essential that the Government not use legitimate threats to computer security as a justification for assuming new powers of regulation or imposing new burdens on industry. New Government controls, technology mandates, or federally imposed standards will not lead to better cyber security. Instead, they would stifle innovation and harm the very infrastructure that needs protection.

The Government also should not use legitimate threats to computer security as a justification for threatening privacy rights. The Government must not increase widespread monitoring of Americans, as we proposed in the original FIDNET plan. We fully support giving law enforcement the requisite resources and training to investigate and prosecute cyber crime. But just because we know someone will commit cyber crime, it is not appropriate to closely watch what everyone is doing.

Chairman Hatch, you and other members of the committee have introduced legislation addressing different aspects of cyber crime and critical information infrastructure protection. As we explained, there are some positive steps that could be taken, but there is no need to rush forward with legislation. Hearings such as these are essential to examine these complex issues. Indeed, ACP has questions and concerns about several aspects of this bill.

For example, we support the funding, as Mr. Vatis asked for, in terms of the FBI and Justice and training personnel with technological capabilities. But we have serious concerns about some of the bill's direction and the duties that are given to the FBI. They are quite expansive and include setting standards as well, which we do not think is appropriate.

I would be pleased to answer any further detailed questions.

[The prepared statement of Mr. Heiman follows:]

## Prepared Statement of Bruce J. Heiman

### I. INTRODUCTION AND SUMMARY

My name is Bruce Heiman, and I am Executive Director of Americans for Computer Privacy (ACP). ACP is a broad-based coalition that brings together more than 100 companies and 40 associations representing high-tech, telecommunications, manufacturing, financial services and transportation, as well as law enforcement, civil-liberties, pro-family, taxpayer groups, and over 6000 individuals. Our members created ACP to focus on issues at the intersection of electronic information and communications, privacy rights, law enforcement, and national security. A list of our membership is attached to my testimony.

Encryption is an essential component of information security. ACP supports policies that advance the rights of American citizens to encode information without fear of government intrusion, and advocates the lifting of export restrictions on U.S.-made encryption products. The Administration's January 14th policy announcement represents a substantive improvement over the prior encryption export policy and a significant movement toward leveling the playing field between U.S. and foreign manufacturers of encryption products. ACP wishes to express its gratitude to the Congress and the Administration for its far-sighted support for liberalization of U.S. encryption export policy.

But more needs to be done. Protecting the critical information infrastructure is essential for U.S. national security, American economic welfare, and our fundamental freedoms.

ACP strongly believes that a voluntary cooperative partnership between government and industry is the only approach that can succeed in protecting critical information infrastructure. ACP supports policies that promote industry-led, market driven solutions to Critical Information Infrastructure Protection and opposes government efforts to impose mandates or design standards. ACP supports giving government the resources necessary to protect its own computer systems, to recruit and train computer security and law enforcement personnel, and to strengthen the government's technological capabilities to investigate and prosecute cyber crime. But ACP opposes government proposals to increase widespread monitoring or surveillance.

Importantly, ACP believes that the government must proceed cautiously and should not rush to pass new legislation. We are concerned about the possibility of overreaction to recent denial of service attacks and Internet viruses. Such an overreaction could generate new laws or regulations which would stifle innovation, harm the very infrastructure that needs protection, and threaten the privacy rights of Americans at work and at home. (ACP has formulated five principles that should structure the current debate concerning Critical Information Infrastructure Protection, which are also attached to my testimony.)

### II. ENCRYPTION IS AN ESSENTIAL COMPONENT OF INFORMATION SECURITY

Encryption is the essential technological ingredient that can ensure the confidentiality, privacy, and authenticity of information. Encryption helps prevent cyber crime and promotes our national security. During the last two years, ACP led the private-sector's effort to permit the widespread use of strong American encryption products in order to protect privacy, promote national security, and prevent crime. With strong Congressional support, we succeeded in persuading the Administration to relax export controls on encryption products.

We commend the Administration on its change in encryption export policy. However, the Administration still requires both licensing and a classification and technical review process for encryption exports. Furthermore, the Administration lacks sufficient resources to meet the nearly 200% increase in classification requests for encryption exports. Despite the new regulations, a lack of government resources results in delayed processing of applications and creates a de facto competitive disadvantage for U.S. companies vis-à-vis their foreign competitors.

Companies of the European Union (EU) will enjoy a further advantage over American companies in world markets due to the EU's recently announced liberalization of its encryption export control policy. The EU essentially created a license-free zone for EU members and another ten countries. In contrast, the United States still requires U.S. companies to apply for licenses to export encryption to foreign countries, except Canada.

On May 15th ACP filed comments urging the Administration to respond to the recent EU encryption export policy. ACP urged the Administration to extend Canada-type treatment to encryption exports to the EU countries and the other countries covered by the EU's new rules. We look forward to working with the Adminis-

tration to prevent U.S. encryption exporters from being disadvantaged by the EU's new policy.

ACP also continues to oppose any efforts by foreign governments to erect import barriers to American products or to impose domestic controls on the use of encryption. We appreciate the Administration's actions, again with strong Congressional support, in opposition to proposed controls in China and France. Overall, we anticipate the widespread use of encryption in the years ahead.

### III. BUT MORE NEEDS TO BE DONE TO PROTECT OUR CRITICAL INFRASTRUCTURE

Technology has made many of our Nation's essential services enormously more robust and reliable. Our information infrastructure has sparked the dramatic increases in productivity underlying the phenomenal economic success story of the 1990's yet the same "interconnectedness" that allows us to increase efficiency and productivity and opens new frontiers of commerce also gives rise to increased vulnerability. All members of ACP are affected by this new vulnerability.

As a result, ACP takes extremely seriously the need for increased cyber-security throughout those sectors of our economy—such as utilities, banking, communications, transportation, healthcare, and e-commerce—that today are so reliant on information systems. The U.S. government, including our national defense establishment, also relies heavily on private-sector networks, products, and services.

The denial of service attacks earlier this year, and most recently the Melissa and Love Bug viruses and their progeny, remind us of the need to secure the information systems on which so many sectors of our economy rely.

ACP's members are working hard to improve computer security and to make the Internet a safe and reliable environment for business and personal use, while preserving the dynamic growth and rapid pace innovation that have made the Internet such an amazing phenomenon.

### IV. A VOLUNTARY COOPERATIVE PARTNERSHIP BETWEEN GOVERNMENT AND INDUSTRY IS THE ONLY APPROACH THAT CAN SUCCEED

In the United States, it is the private sector that develops, owns, operates and maintains the networks, systems, products, and services that make up the information infrastructure. It also is the private sector that possesses the knowledge and expertise necessary to protect it.

So far, the Administration—in Presidential Decision Directive 63, the National Plan for Information Systems Protection, Version 1.0, and various other activities—has recognized that it should work cooperatively with industry on a voluntary basis to deter, identify, and respond to cyber threats and attacks.

Both the private sector and the government play key roles in Critical Information Infrastructure Protection.

*What should the private sector be doing?*

*First,* what information technology companies already have been doing for some time: constantly improving protection in their product lines and networks. Information and communication sector companies accept that improved network and information systems security is imperative, and they are willing to do their part.

Private companies are in the best position to know how to protect infrastructures they have developed, owned and operated. But it is important to understand that there is no one single "silver bullet" for the problem of information security—rather, it is a *process* of continual improvement.

*Second,* it is incumbent upon all of us to practice good "security hygiene" and to educate others to do so. For example, many people choose a password that is related to something about them and thus make it easier to figure out. Also, many people do not change their passwords at regular intevals. Others simply choose an English language word rather than a random sequence of letters, symbols, and numbers, which is far more difficult to crack.

Perhaps the recent Internet virus attacks have had a positive effect: all of the attention on Internet viruses has made computer users more wary and less trusting. According to a recent Pew Internet and American Life Project poll reported in the *Washington Post,* only about 25% of users who received the Love Bug email attachment actually opened it. This is a real improvement. The private sector needs to continue to spread the message that, just as you wouldn't let anybody into your house, so you shouldn't let just anybody into your computer.

*Third,* industry does need to share information among itself and with the government about threats and vulnerabilities as well as best practices. In this regard, ACP has met with representatives of the National Security Council staff, the FBI's National Infrastructure Protection Office (NIPC), and the Dept. of Commerce's Critical

Infrastructure Assurance Office (CIAO), and ACP has been encouraged to continue the dialogue. Furthermore, several of ACP's members will be serving on the President's National Infrastructure Assurance Council, a CEO-level group that is being formed to advise the President and Cabinet members. Many of ACP's members are also active participants in the Partnership for Critical Infrastructure Security, a cross-sector, cross-industry effort supported by Commerce Secretary Daly and John Tritak, Director of the Critical Infrastructure Assurance Office (CIAO). The Partnership has already met a number of times and established several working groups.

There is an ongoing, serious discussion within industry itself and between industry and government about the possible need for legislation to facilitate the sharing of information among the private sector and between the private sector and government. Such legislation could provide enhanced protection for shared information by removing disincentives for this dialogue imposed by antitrust laws and FOIA requirements and resulting from the apparent ability of third-parties to use such disclosed information against those who provide it.

*Of course, the government also has an essential role to play as well*

*First,* it is important for the government to share information with the private sector. This includes alert warnings of particular threats. We are encouraged in this regard by the approach taken and attitudes shown by the FBI's National Infrastructure Protection Center. However, we think the government needs to keep improving the time it takes from receiving information to issuing an alert.

*Second,* it is important the government leads by example and gets its own house in order. In this regard, it does appear that the government needs to continue improving as well. The Love Bug virus affected government computers, and the GAO recently criticized the vulnerability of the Executive Branch to the recent virus attacks.

*Third,* we strongly support law enforcement's efforts to increase training of officers, including at the state and local levels, in the detection and prosecution of cyber crime. ACP supports funding to hire and train additional government computer security personnel. We also will continue to work with law enforcement to educate their people.

*Fourth,* we support strengthening the government's technological capabilities to investigate and prosecute cyber crime. Law enforcement needs to have the same state-of-the-art hardware and software possessed by criminal hackers. ACP supports additional appropriations so that law enforcement has the tools to counter the threat posed by these hackers. We also will continue to work with law enforcement so that government can better understand the technology.

*Fifth,* we support the idea of new cyber security scholarships and the creation of a new "cyber corps" of those with specialized educations in the prevention, detection, investigation, and prosecution of cyber crimes and in the protection of our critical infrastructure. Today, there are not enough academic centers offering curricula in cyber security. Government and the private sector should join together to incubate such schools in order to develop tomorrow's leaders in cyber security.

## V. GOVERNMENT MUST PROCEED CAUTIOUSLY

While Critical Information Infrastructure Protection is very important to both the private-sector and the government, ACP also believes it is important that government not overreact to the recent denial-of-service attacks and Internet viruses. Indeed, precipitous action can do far more harm than good.

*First,* it is important to remember that Internet viruses such as the Love Bug are not a new problem and in fact represent a complex, variegated problem. To be more specific, according to the *Washington Post,* information technology companies have identified roughly 40,000 different viruses, including 29 separate versions of the Love Bug. Information technology companies constantly upgrade their products and support services to provide protection against similar attacks. Indeed, only private companies—as opposed to the government—have the quickness and agility to stay abreast of the rapidly developing technology of cybersecurity.

*Second,* information technology companies are responding with greater rapidity to such attacks. It is usually only a matter of hours before a virus has been detected and analyzed and a software patch fixing the problem is posted on the Internet for free download. Thus, according to many calculations, the response to the Love Bug virus was much quicker than the response to the Melissa virus.

*Third,* the public *is* becoming better educated about "security hygiene." The recent Pew Poll reported in the *Washington Post* is encouraging: only one in four recipients of the Love Bug virus actually opened the attachments in the face of widespread dissemination about the dangers of the virus. We believe that individuals at home and at work are beginning to evaluate critically the messages and information they

receive and to take seriously their security responsibilities—whether it be changing their passwords, using better encryption, or updating their anti-virus software.

*Fourth,* there is little doubt that true cyber crime is illegal under our existing laws and that such crimes could be prosecuted. Moreover, private sector individuals with particular expertise have, and will continue to, cooperate with and assist law enforcement in investigating and prosecuting cyber criminals. I should note that ACP does not think it appropriate or desirable to use the possible absence of sufficient laws in other countries to enact new legislation in the United States that might infringe on privacy rights.

*Fifth,* we strongly believe that new government controls, technological mandates, or federally imposed standards will *not* lead to better Critical Information Infrastructure Protection. It is essential that the government not use legitimate threats to computer security as a justification for assuming new powers of regulation, imposing new burdens upon industry, or mandating that the private sector use particular technologies or processes. Such commands would backfire by stifling innovation, artificially channeling R&D, and harming the very infrastructure that needs protection.

*Sixth,* government must not violate personal and corporate privacy in the quest for Critical Information Infrastructure Protection. Once again, the government should not use legitimate threats to computer security as a justification for threatening fundamental rights of privacy. Indeed, as more of our lives are conducted electronically, it is essential that we ensure the security and privacy of information, communications, and transactions that dominate our daily lives from unjustified and unwarranted government examination. The government must not increase widespread surveillance or monitoring of Americans at home and work. While we fully support giving law enforcement the requisite resources and training to investigate and prosecute cyber crime, it is quite another thing to say that, just because *some* will commit cyber crime, it is necessary to watch closely what *everyone* is doing.

One example of this danger is the government's original plan for FIDNET—the Federal Intrusion and Detection Network. As originally conceived, the Administration proposed that the FBI monitor Internet traffic generally within this country. We are pleased that, in response to widespread Congressional and private sector criticism, the Administration has changed FIDNET's mission to be, more appropriately, one of monitoring the federal government's *own* computer networks. This is much more in line with what companies do in terms of monitoring their own information systems and it is something quite concrete, which can improve information security. However, troubling proposals keep bubbling up. The *Washington Post* recently reported on the FBI's plan to build a "casa de web" data mining computer system for recording and analyzing Internet activity.

Chairman Hatch, you and Senator Leahy and other members of the committee have introduced legislation addressing different aspects of cyber crime and critical infrastructure protection. As we have explained, there are some positive steps that could be taken. But there is no need to rush forward with legislation. Indeed, ACP has questions and concerns about several aspects of these bills (*e.g.,* the proper role of the FBI's NIPC, international cooperation standards, and the extension of trap and trace devices and pen registers to electronic communications). This area is both legally and technologically complex. Hearings such as these are essential. ACP believes that at this point much legislation concerning Critical Information Infrastructure Protection is in fact premature.

## VI. CONCLUSION

Thank you again for this opportunity to testify. ACP believes there is much for the private sector and the government to do *together,* and ACP looks forward to working with the government to protect our critical infrastructure and thus our economy, national security, and fundamental freedoms.

---

## AMERICANS FOR COMPUTER PRIVACY MEMBERSHIP LIST

### ASSOCIATIONS

60 Plus Association, American Conservative Union, American Electronics Association, American Financial Services Association, American Petroleum Institute, American Privacy Protection Association, American Small Business Alliance, Americans for Tax Reform, Business Software Alliance, Cellular Telecommunications Industry Association, Center for Democracy and Technology, Citizens for a Sound Economy, Commercial Internet eXchange Association, Computer and Communications Indus-

try Association, Computing Technology Industry Association, Consumer Electronics Manufacturers Association, Eagle Forum, Electronic Commerce Forum, Electronic Industries Association, and FTD Association.

Information Technology Association of America, Information Technology Business Center, Information Technology Industry Council, Interactive Services Association, IEEE–USA, Law Enforcement Alliance of America, Louisiana Sheriffs' Association, NASDAQ, National Association of Manufacturers, National Retail Federation, National Rifle Association, National Venture Capital Association, Online Banking Association, Securities Industry Association, Small Business Survival Committee, Software Publishers Association, Telecommunications Industry Association, U.S. Chamber of Commerce, and U.S. Telephone Association.

COMPANIES

3Com Corporation, 3K Associates, Incorporated, ACL Datacom, Incorporated, Acordia Northwest, Incorporated, Adobe Systems, Incorporated, Altopia Corporation, America Online, Incorporated, Asia Pacific Marketing, Incorporated, Autodesk, AXENT Technologies, Incorporated, BEA Systems, Inc., Bell South, Bokler Software Corporation, Bowles Farming Company, Brooks Internet Software, Incorporated, Central Predicting Corporation, Centurion Soft, Cipher Logics Corp., Circuit City, and Cisco Systems, Incorporated.

Citrix Systems, Incorporated, Claris Corporation, CommerceNet, Compaq Computer Corporation, Computer Associates International Incorporated, Consensus Development Corporation, Corel Corporation, Countrywide Home Loans, Inc., DAK, DBA Springfield CyberLink, deregulation.net, EDS Corporation, Envision, Incorporated, Furukawa Information Technologies, Inc., General Instrument Corporation, Genio USA, GeoData Solutions, Incorporated, Geoworks, GFI Consulting, and Goodyear Tire & Rubber Company.

Honeywell, Incorporated, I.S. Grupe Incorporated, I/O Software, Incorporated, Intel Corporation, Intellectual Protocols, LLC, Intellimedia Commerce, Incorporated, Intershop Communications, Incorporated, Intersolv, Incorporated, Intuit, Incorporated, Invincible Data Systems, Incorporated, Kapenda Corp., Kellogg Technologies, Kinesix Corporation, Lehrer Financial and Economic Advisory Svcs., Litigation Support Systems, Lotus Development Corporation, Lucent Technologies, Mac Sourcery, Mastercard International, Incorporated, and McLellan Software Center, Incorporated.

MeterNet Corporation, Microsoft Corporation, Microtest, Incorporated, Mindscape, Incorporated, Napersoft, Incorporated, NeoMedia Technologies, Incorporated, Netscape Communications Corporation, Network Associates, Network Risk Management Services, Nokia, Novell, Incorporated, Now Software, Incorporated, Oracle Corporation, Piranha Interactive Publishing, Incorporated, Platinum Technology, Incorporated, Portland Software, Incorporated, ProSys, Incorporated, Rail Safety Engineering, Incorporated, Raptor Systems, Inc., and Raycom Data Technologies, Incorporated.

ReCor Corporation, Red Creek, Rockwell International, RSA Data Security, Incorporated, Santa Cruz Operation, Incorporated, SAS Institute, Inc., SBC Telecommunications, Inc., Secure Computing Corporation, Shadow Technologies, Silenus Group, Silicon Valley Software Industry Coalition, SISCO, Inc., SkillsBank Corporation, Soft Machines, Soundcode, Inc., Southern Company, Storage Technology Corporation, Sun Microsystems, Incorporated, and Sybase, Incorporated.

Symantec Corporation, SynData Technologies, SynData Technologies, Target Printing & Graphics, Ultimate Privacy Corporation, UUNet Technologies, Visa International, Vortex Solutions, Watchguard Technologies, Inc., and Wyatt River Software, Incorporated.

---

AMERICANS FOR COMPUTER PRIVACY 2000 STATEMENT OF PRINCIPLES

ACP strongly believes that protecting the global information infrastructure ("critical information infrastructure protection" or "CIIP") is essential for U.S. national security, American economic welfare, and our fundamental freedoms. ACP has adopted the following five principles:

1. CIIP is best accomplished through private sector solutions that are market driven and industry led. The private sector owns, operates, and has developed the networks and services that constitute the information infrastructure.

2. Governments and industry must work cooperatively on a voluntary basis towards achieving CIIP. This should include an institutionalized and thoughtful dialogue between key government officials and industry.

3. Government must not mandate the private sector use of particular technologies or processes, dictate standards, or increase widespread surveillance or monitoring of citizens at home and work under the banner of CIIP.

4. Governments must not violate personal and corporate privacy in the quest for CIIP. Such privacy protection is best preserved by scrutiny of new governmental CIIP authority.

5. Barriers to strong CIIP should be removed, including barriers to the widespread use of strong encryption. Encryption promotes national security, prevents crime, and protects privacy. The U.S. Government must fully implement the recent relaxation in U.S. encryption export controls and make additional changes as necessary to ensure the ability of American companies to lead globally. Governments must not impose foreign import barriers or domestic controls.

The CHAIRMAN. Thank you very much.

Mr. Pethia, we will turn to you.

## STATEMENT OF RICHARD PETHIA

Mr. PETHIA. Mr. Chairman, Senator Feinstein, thank you for the opportunity to testify on security issues. My perspective comes from the work that we do at the CERT coordination center, established in 1988 by the Defense Advanced Research Projects Agency to respond to Internet security emergencies and to help prevent future incidents. Since then, we have handled over 28,000 separate security incidents and analyzed more than 1,500 vulnerabilities in network-related products. Over 80 incident response teams around the world have adopted our incident handling practices.

When a security breach occurs, our staff members help the administrators of the affected sites to identify and correct the vulnerabilities that allowed the incident to occur. We issue advisories to the Internet community warning of serious security threats. We are responsible for the day-to-day operations of the Federal computer incident response capability, an organization operated by the General Services Administration that provides direct support for the Federal civil agencies. We also handle reports of vulnerabilities in commercial products, and work with technology producers to fix them.

The vulnerabilities that we see on the Internet put government, business, and individual users at risk. The current state of security is the result of many factors. Rapid growth of the Internet brings new users who are not aware of security issues. As the technology is being distributed, so is the management of that technology. System administration and management often fall upon people who do not have the training, skills, resources, or interest needed to operate their systems securely.

The Internet is becoming increasingly complex, and with that complexity comes increased vulnerability. When vendors release upgrades to solve security problems, organizations often do not upgrade their systems. The job may be too time-consuming, too complex, or just too low a priority for the system administration staff to handle. There is little evidence of security improvement in most new products. Developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerability.

Finally, engineering for ease of use is not being matched by engineering for ease of security and administration. Products are very easy to use, but they are very difficult to secure. This is a dynamic problem. The Internet and other forms of communications systems will continue grow and interconnect. More and more people will

conduct business and become otherwise dependent on these networks. More and more people will lack the detailed technical knowledge and skill that is required to effectively protect systems. More and more attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain.

The network technology will evolve, and the attack technology will evolve right along with it. Many of the solutions that work today won't work tomorrow. To move forward, we need to make improvements to existing capabilities, but also make fundamental changes to the way technology is developed, packaged, and used.

We need, and your bill supports, enhanced response capabilities to keep up with the new forms of attack. New forms of communications must be developed that provide system operators with near realtime access to information about security events. The mechanisms that we have today work in units of hours and days, but the kinds of attacks that we will see in the future won't give us that luxury. We will need to move much more quickly.

In the long term, it is unrealistic to expect that response organizations and system administrators, even with highly automated procedures, will be able to stay ahead of the kinds of automated attacks we can expect to see in the future. At the same time, the average level of technical understanding of system users is declining, and that trend will continue. In this environment, a security approach based on "user beware" is unacceptable.

The long-term solution requires a combination of virus-proof software. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Vendors must provide systems and software that are virus-resistant.

Widespread use of encryption and strong authentication. Many forms of attack are successful partly because attackers are able to masquerade as being someone that the attack target knows. Widespread deployment of strong authentication technology will help us deal with that problem.

High-security default configurations. Properly configuring systems and networks to use the strongest security built into products is difficult. Vendors can help reduce the impact of security problems by shipping products with configurations that enable security options rather than requiring the user to enable them.

In the end, response techniques can go just so far in limiting damage, and we are approaching the limits. It is critical that system operators and product developers recognize that their systems and products are now operating in hostile environments. Operators must demand and developers must produce products that are fit for use in this environment.

With respect to the new legislation, we very much support the increased resources for the NIPC and their role of incident response, but would encourage you to consider looking at allocating at least some of those funds toward increased roles in prevention for the Justice Department and for others in the Federal Government. Until we begin to build stronger foundations in our technology base, we are going to have a problem that will be very difficult to deal with. We won't have enough resources to deal with

the reactive side of the problem, and we need more focus on preventing the problem to begin with.

Thank you.

[The prepared statement of Mr. Pethia follows:]

PREPARED STATEMENT OF RICHARD PETHIA

INTRODUCTION

My name is Richard Pethia. I manage the Survivable Systems Initiative and the CERT Coordination Center (CERT/CC) at Carnegie Mellon University's Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania.

Thank you for the opportunity to testify on the role of the CERT/CC in dealing with Internet security issues. Today I will give some background on the CERT/CC, describe our experience with Internet security incidents, and outline some of the steps that I believe must be taken to reduce the impact of future security incidents.

BACKGROUND

The CERT Coordination Center (CERT/CC) is located at the Software Engineering Institute (SEI), a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Internet Worm incident, which brought 10 percent of Internet systems to a halt in November 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. Since then, the CERT/CC has handled over 28,000 computer network security incidents and analyzed more than 1,500 vulnerabilities in network-related products. Over 80 incident response teams around the world have adopted the incident handling practices of the CERT/CC.

Today, the Defense Information Systems Agency, the General Services Administration, and the Federal Bureau of Investigation sponsor the CERT/CC's work. The CERT/CC provides assistance to computer system administrators in the Internet community who report security problems. When a security breach occurs, CERT/CC staff members help the administrators of the affected sites to identify and correct the vulnerabilities that allow the incident to occur. The CERT/CC staff also coordinates the response with other sites affected by the same incident. When a site specifically requests, CERT/CC staff members facilitate communication with law enforcement agencies.

The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form incident response teams and provides guidance to newly formed teams. The CERT/CC is also responsible for the day-to-day operations of the FedCIRC (Federal Computer Incident Response Capability) Operations Center, an organization that provides incident response and other security-related services to Federal civilian agencies. The General Services Administration (GSA) manages FedCIRC.

The CERT/CC also handles reports of vulnerabilities in commercial products. When we receive a vulnerability report, our vulnerability experts analyze the potential vulnerability and work with technology producers to inform them of security deficiencies in their products and to facilitate and track their response to these problems. Another source of vulnerability information comes from incident analysis. Repeated incidents of the same type often point to the existence of a vulnerability and, often, the existence of public information or automated tolls for exploiting the vulnerability. To achieve long-term benefit from vulnerability analysis, we have begun to identify the underlying software engineering and system administration practices that lead to vulnerabilities and, conversely, practices that prevent vulnerabilities.

Our ongoing computer security incident response activities help the Internet community to deal with its immediate problems while allowing us to understand the scope and nature of the problems and of the community's needs. Our understanding of current security problems and potential solutions comes from first-hand experience with compromised sites on the Internet and subsequent analysis of security incidents, intrusion techniques, configuration problems, and software vulnerabilities.

As a result of our incident and vulnerability analysis work, we have a broad view of incident and vulnerability trends and characteristics. We communicate this information back to the community through online reports, presentations at conferences and workshops, and training courses. In addition critical information about specific threats goes out to the Internet community through security alerts such as CERT

advisories, incident notes, vulnerability notes, and vendor-initiated bulletins. The government receives early warnings through "special communications" to the Department of Defense (through their incident response teams), Federal civil agencies (through FedCIRC), and the FBI. This work is possible because the CERT/CC has become a major reporting center for incidents and vulnerabilities because staff members have an established reputation for discretion and objectivity. As a result of the community's trust, and receive thousands of reports every year.

In addition to incident response and vulnerability handling, we also work on security improvement and network survivability.

In the area of security improvement we are defining security improvement practices to provide concrete, practical guidance that will help organizations improve the security of their networked computer systems. These practices are being published as security improvement modules and focus on best practices that address important problems in network security. We also transition these practices through courses offered by the SEI and by the SEI's transition patterns.

Our staff members are also developing a comprehensive, repeatable technique for identifying vulnerabilities in networked systems through self-evaluation. The information security self-evaluation takes into consideration policy, management, administration, and other organizational issues, as well as technology, to provide a comprehensive view of the information security state of an organization. We see this evaluation method as a key component of an overarching security improvement framework that allows an organization to maintain an acceptable level of security by quickly adapting to changes in the internal and external environments.

In the area of network survivability, we are concentrating on the technical basis for identifying and preventing security flaws and for preserving essential services in the event of intrusions, accidents, or failures. This work draws on the incident data collected by the CERT/CC. We are developing a survivable network analysis method, which uses a structured architectural specification of an existing or proposed network application to determine the most likely points in the architecture where accidents and/or intrusions could cause the mission of the application to fail. This method leverages SEI expertise in risk and architectural analysis, network intrusion expertise, and vulnerability analysis. It is applied to a selected system by a SEI assessment team working with system architects and stakeholders. survivable network analysis identifies essential services and assets of the application that must survive intrusion, evaluates its ability to withstand attack, and recommends architecture strategies to mitigate vulnerabilities that are uncovered. The method is designed to scale to highly distributed systems in unbounded domains such as the Internet, for which traditional security techniques are inadequate. Along with the analysis method, our staff is building a simulator to explore survivability characteristics of large networked applications in an environment of limited administrative control. This will enhance the analysis of national infrastructures dependent on information systems that are interconnected and interdependent. This simulator will be used as part of a more advanced analysis technique for networked applications and network protocols. The simulator will help us understand how cascade effects and other complex failures arise from large networked domains where administrative control is localized but there is a dependence on network elements beyond this administrative control.

VULNERABILITY OF THE INTERNET AND WORLD WIDE WEB

Vulnerabilities associated with the Internet put government, business and individual users at risk. Security measures that were appropriate for mainframe computers and small, well-defined networks inside an organization are not effective for the Internet, a complex, dynamic world of interconnected networks with no clear boundaries and no central control. Because the Internet was not originally designed with security in mind, it is difficult to ensure the integrity, availability, and privacy of information. The Internet was designed to be "open," with distributed control and mutual trust among users. As a result, control is in the hands of users, not in the hands of the provider; and a central authority cannot administer use. Furthermore, security issues are not well understood and are rarely given high priority by software developers, vendors, network managers, or consumers.

In addition, because the Internet is digital, not physical, it has no geographic location and no well-defined boundaries. Traditional physical "rules" are difficult or impossible to apply. Instead, new knowledge and a new point of view are required to understand the workings and the vulnerabilities of the Internet.

Another factor is the approach typically taken by the intruder community. There is (loosely) organized development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, in-

truders take an open-source approach to development. One can draw parallels with open system development: there are many developers and a large, reusable code base.

Intruder tools are becoming increasingly sophisticated and also becoming increasingly user friendly and widely available. For the first time, intruders are developing techniques to harness the power of hundreds of thousands of vulnerable systems on the internet. Using what are called distributed-system attack tools, intruders can involve a large number of sites simultaneously, focusing all of them to attack one or more victim hosts or networks. The sophisticated developers of intruder programs package their tools into user-friendly forms and make them widely available. As a result, even unsophisticated intruders can use them.

The current state of Internet security is the result of many additional factors, such as the ones listed below. A change in any one of these can change the level of Internet security and survivability.

- Because of the dramatically lower cost of communication on the Internet, use of the Internet is replacing other forms of electronic communication. The Internet itself is growing at an amazing rate, as noted in an earlier section.
- There is a continuing movement to distributed, client-server, and heterogeneous configurations. As the technology is being distributed, so is the management of that technology. In these cases, system administration and management often fall upon people who do not have the training, skill, resources, or interest needed to operate their systems securely. The number of directly connected homes, schools, libraries and other venues without trained system administration and security staff is rapidly increasing. These "always-on, rarely-protected" systems allow attackers to continue to add new systems to their arsenal of captured weapons.
- Internet sites have become so interconnected and intruder tools so effective that the security of any site depends, in part, on the security of all other sites on the Internet.
- The difficulty of criminal investigation of cybercrime coupled with the complexity of international law mean that successful apprehension and prosecution of computer criminals is unlikely, and thus little deterrent value is realized.
- The Internet is becoming increasingly complex and dynamic, but among those connected to the Internet there is a lack of adequate knowledge about the network and about security. The rush to the Internet, coupled with a lack of understanding, is leading to the exposure of sensitive data and risk to safety-critical systems. Misconfigured or outdated operating systems, mail programs, and Web sites result in vulnerabilities that intruders can exploit. Just one naive user with an easy-to-guess passwork increases an organization's risk.
- When vendors release patches or upgrades to solve security problems, organizations' systems often are not upgraded. The job may be too time-consuming, too complex, or just at too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.
- As we face the complex and rapidly changing world of the Internet, comprehensive solutions are lacking. Among security-conscious organizations, there is increased reliance on "silver bullet" solutions, such as firewalls and encryption. The organizations that have applied a "silver bullet" are lulled into a false sense of security and become less vigilant, but single solutions applied once are neither foolproof nor adequate. Solutions must be combined, and the security situation must be constantly monitored as technology changes and new exploitation techniques are discovered.
- There is little evidence of improvement in the security features of most products; developers are not devoting sufficient effort to apply lessons learned about the sources of vulnerabilities. The CERT Coordination Center routinely receives reports of new vulnerabilities. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on security features. Until their customers demand products that are more secure, the situation is unlikely to change.
- Engineering for ease of use is not being matched by engineering for ease of secure administration. Today's software products, workstations, and personal computers bring the power of the computer to increasing numbers of people who use that power to perform their work more efficiently and effectively. Products are so easy to use that people with little technical knowledge or skill can install and operate them on their desktop computers. Unfortunately, it is difficult to configure and

operate many of these products securely. This gap leads to increasing numbers of vulnerable systems.

SOLUTIONS

While it is important to react to crisis situations when they occur, it is just as important to recognize that information assurance is a long-term problem. The Internet and other forms of communications systems will continue to grow and interconnect. More and more people and organizations will conduct business and become otherwise dependent on these networks. More and more of these organizations and individuals will lack the detailed technical knowledge and skill that is required to effectively protect systems today. More and more attackers will look for ways to take advantage of the assets of others or to cause disruption and damage for personal or political gain. The network and computer technology will evolve and the attack technology will evolve along with it. Many information assurance solutions that work today will not work tomorrow.

Managing the risks that come from this expanded use and dependence on information technology requires an evolving strategy that stays abreast of changes in technology, changes in the ways we use the technology, and changes in the way people attack us through our systems and networks. To move forward, we will need to make improvements to existing capabilities as well as fundamental changes to the way technology is developed, packaged, and used.

• Enhanced incident response capabilities—The incident response community has handled most incidents well, but is now being strained beyond its capacity. In the future, we can expect to see multiple broad-based attacks launched at the Internet at the same time. With its limited resources, the response community will fragment, dividing its attention across the problems thereby slowing progress on each. In addition, system operators will be confused as they try to understand if they are dealing with one problem with multiple symptoms or with multiple, simultaneous problems. New forms of communications must be developed that provide system operators with near real-time status on network security events with less person-to-person interaction than is required today. Incident response organizations must develop more effective ways to analyze security events and vulnerability data and to disseminate the results of the analysis to their constituents quickly. The mechanisms we have today work in units of hours and days, more time than we will have when faced with widespread, rapidly moving problems.

• Changes in technology development, packaging and use—In the long-term, it is unrealistic to expect that response organizations and system administrators, even with highly automated procedures, will be able to stay ahead of problems that move at Internet speed. While response teams will always be needed to handle new threats and unprecedented situations, technology producers must recognize that their products are being used in hostile environments and take steps to insure that their products are fit for use in those environments. Computers and software are becoming more powerful and more interconnected. At the same time, the average level of technical understanding of system users is declining. Powerful computers and software that anyone and everyone can use, without having a deep understanding of the technology, are now available. In this environment, a security approach based on "user-beware" is unacceptable. The systems are too complex for this approach to work. The long-term solutions required are a combination of the following.

• Virus-resistant/proof software—There is nothing intrinsic about digital computers or software that makes them vulnerable to virus attack or infestation. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs that allow the import of executable code, in one form or another, and allow the unconstrained execution of that code on the machine that received it, are the designs that are susceptible to viruses and their effects. Unconstrained execution allows code developers (e.g. macro-code developers) to take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or not-trusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, have been more recently developed.

• Widespread use of strong authentication—Many forms of attack are successful partly because attackers are able to masquerade (in either direct attacks or indirect attacks launched through viruses) as being someone that the attack target knows. Carefully implemented authentication technology, such as digital signatures, that is in widespread use would allow people to reject messages, documents and code from

unknown sources. This would have an immediate impact of inhibiting the spread of email carried viruses. Strong cryptographic technology exists today to provide integrity and authentication, but it is not in widespread use. Widespread deployment will require secure, manageable key distribution infrastructures and research and development to produce these infrastructures should be accelerated.

• High-security default configurations—With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills training. Small mistakes can leave systems vulnerable and put users at risk when connected to the Internet. Vendors can help reduce the impact of security problems by shipping products with configurations that enable security options rather than require the user to enable them. The user can lower these "default" configurations if desired, but should provide the best security possible unless the user takes explicit steps to reduce it.

CONCLUSION

The recent rash of attacks on the Internet demonstrates how quickly automated attacks can spread across the network and hints at the kind of damage that can be done. Incident response organizations are able to limit damage by working effectively together to analyze the problem, synthesize solutions, and alert the community to the need to take corrective action. With the attacks we can expect to see in the future, response organizations will need expanded resources and new techniques to act quickly and effectively. Response organizations will always have a role to play in identifying new threats and dealing with unprecedented problems, but response methods will not be able to react at Internet Speeds with complicated viruses or with multiple simultaneous attacks of different types.

The long-term solutions to the problems represented by new forms of automated attack will require fundamental changes to the way technology is developed, packaged and used. It is critical that system operators and product developers recognize that their systems and products are now operating in hostile environments. Operators must demand, and developers must produce, products that are fit for use in this environment. As new forms of attack are identified and understood, developers must change their designs to protect systems and networks from these kinds of attack.

The CHAIRMAN. Thank you, Mr. Pethia.

Mr. Richards, we will turn to you.

## STATEMENT OF JEFF B. RICHARDS

Mr. RICHARDS. Mr. Chairman, Senator Feinstein, I am Jeff Richards, Executive Director of the Internet Alliance. We were founded in 1982. Sometimes people think that is a typo. Actually, we were the Videotech Industries Association, the only trade association to address online and Internet issues from a consumer Internet online perspective. In fact, we were that group of 50 people who said in 1982–1983 there will be a consumer online marketplace one day, and when there is, it will change everything. That is what we are talking about today.

Our mission is to increase consumer trust and confidence in the Internet by promoting good business practice, public education initiatives, enforcement of existing laws protecting consumers, and development of a legal framework governing the Internet that will provide, at the same time, predictability, efficiency, security, and freedom to innovate.

In particular, I will focus on security matters, coming as I did from last week's G–8 meeting in Paris, during which we released the Internet Alliance's white paper which is entitled "An International Policy Framework for Internet Law Enforcement and Security." Mr. Chairman, I would like to have the white paper, if possible, appended to my remarks for the record.

The CHAIRMAN. Without objection, we will do that.

[The white paper follows:]

## An International Policy Framework for Internet Law Enforcement and Security: An Internet Alliance White Paper, May 2000

### EXECUTIVE SUMMARY

In its short life, the Internet has helped us realize the great potential of the information age. We are just now beginning to reap the economic and social benefits from cyberspace. However, as a value-neutral technological tool, the Internet has also brought new forms of crime and new ways to commit traditional crime. Thus, today, as the Internet enters its adolescence, it is a very sensitive time in which it is essential for its users to have a sense of confidence and trust in this new medium.

Recent events including "distributed denial of service attacks" on major Web sites and outbreaks of Internet-spread computer viruses have raised international concern and highlighted the need for a policy framework to address the issue of Internet crime. As the leading consumer Internet industry association, the Internet Alliance, through public policy, advocacy, consumer outreach and strategic alliances is seeking to build this confidence and trust necessary for the Internet to become a leading global market medium of the 21st Century.

In combating cybercrime, we apply a levelheaded, first-things-first approach and encourage the application of existing laws before rushing to create new ones. Of course, there are many obstacles to effectively enforcing these laws. The Internet knows no borders, thus coordination within nation-states and internationally is problematic. While some such efforts to address this are underway, many more are needed.

At the same time, the Internet is an intensely local and intensely global experience. While it provides for communication over vast distances in cyberspace, its effects can have very real implications upon local communities and individual users. Thus, while there is an immediate need to coordinate international efforts in combating Internet crime, such initiatives should also incorporate national and local law enforcement authorities. Without effective law enforcement at all levels of government, gaps in coverage could lead to overall ineffectiveness.

Thus far, law enforcement has not been able to keep up with technology moving at "Internet time." Lacking the resources and experience, especially at the local level police agencies are struggling to keep up with the increasing level of cybercrime. While the Internet industry is well positioned to help, industry cooperation in assisting law enforcement in investigations should be voluntary and in strict compliance with existing law.

With the help of groups such as the Internet Alliance, industry can assist in the training and education of law enforcement officials and help them to train themselves. Industry should also come together in forums such as the IA's Law Enforcement and Security Council to share best business practices, form flexible standards, and offer new initiatives in the global effort to fight cybercrime. Recognizing that education is the best form of prevention, industry should also work to promote educational initiatives not only for law enforcement personnel, but for consumers as well. The cooperation and proactive work of industry should provide good support for law enforcement. This should come voluntarily, motivated by concern for the marketplace. At the same time, the enforcement of law should remain under the domain of government.

Working together in their respective roles, industry, government and empowered consumers will be able to better assess, address and prevent Internet crime. It is our hope that this white paper offers a place from which to start such cooperation and communication. These efforts can only work to further establish the trust and confidence necessary for the Internet's success.

### INTRODUCTION

As the word itself implies, the Internet is a global network of networks, connecting people and relaying information. From e-commerce to chat rooms, the Internet acts as an extension and facilitator of traditional offline economic and social activities that people have conducted for years before the information age. These activities also include traditional unlawful acts such as fraud and identity theft. Like any technology, the Internet is an inherently value-neutral tool and can also be used by criminals as well as consumers. While some criminal acts such as the recent distributed denial of service (DDoS) attacks are unique to the Internet and its technology, most online crime is an "Internet version" of offenses with long histories in the real (not virtual) world. Guided by this principle, the Internet Alliance, in the second of a series of white papers, provides a framework for assessing, addressing, and ultimately preventing Internet crime.

Today, we are just beginning to realize the far-reaching economic and social benefits that the Internet can offer. The Internet Alliance is committed to help our industry build the confidence and trust necessary for the Internet to become the global mass market medium of the 21st century through public policy, industry advocacy, consumer education and media relations. In 1998, the Internet received a permanent place on the agendas of policymakers around the world. On countless fronts, and in a host of ever-expanding issue areas, the Internet is being addressed through hundreds of different policy decisions that will profoundly affect the Internet, consumers and e-commerce. Businesses providing access, content, software and hardware are now seen as a seamless "Internet industry" by policymakers, media and consumers. Yet until a few months ago, representation acknowledging this new, holistic nature of the Internet industry was non-existent. The IA is dedicated to advocating the Internet industry perspective on issues deeply important to both consumers and to business. Drawing upon the knowledge, experience and expertise of the industry members who comprise our Law Enforcement and Security Council (LESC), we address the issue of Internet crime in this greater context and, in doing so, have several guiding themes:

- Policymakers must carefully weigh the complete range of available information before acting on Internet issues, in order to avoid harmful unintended consequences;
- Consumer Internet policy should avoid creating an unpredictable marketplace environment, one where consumers face a "hit-or-miss" electronic shopping experience;
- Policies adopted for the Internet should reflect the importance of consumer choice in the marketplace;
- Policies addressing the consumer Internet must reflect the need to help educate consumers about use of the new medium;
- Technological tools can be and frequently are more effective than government regulations at dealing with social issues related to the Internet;
- Consumer Internet policy must not be rooted in alarmist depictions of the Internet, and policymakers should strive not to let the abusive actions of a few Web sites obscure the unquestioned utility and benefits of the new medium.[1]

It is also important to recognize the efforts of the other national and international bodies who, along with the Internet Alliance, are taking the first steps in defining the issue and working to combat cybercrime. These groups include the G–8, the Council of Europe, INTERPOL, the United Nations, the European Council, the Organization of American States, the US Departments of Justice, Treasury and State, the National White Collar Crime Center, the National Cybercrime Training Partnership, and the National Center for Missing and Exploited Children.

To begin, we will evaluate the nature and scope of law enforcement and security on the Internet. There are various types of crimes being committed online. We identify some of these, not for the purpose of offering specific solutions, but rather for the purpose of determining the context for more general recommendations. In order to address the issue, we must first know what it encompasses.

Most online crime is traditional "offline" crime committed in a new way. Therefore, the primary guiding principle we support in addressing this issue is the application of existing law to offenses committed on the Internet. At the same time, the Net's global coverage presents unique jurisdictional problems. In evaluating these, this paper emphasizes the importance of local level law enforcement and security. While the need for intentional cooperation and coordination in dealing with crimes committed in cyberspace may seem obvious, the local element is less so. With the click of a mouse, Internet users can communicate and send information instantly across the world. Yet, they also exist as citizens in their local communities. And in times of crisis, after a crime has been committed, most turn to their local authorities first. Accordingly, we then explore the best methods for bridging the gaps that exist among international, national, and local law enforcement officials who combat Internet crime.

Not surprisingly, private industry has taken the lead in addressing issues of law enforcement on the Internet. These efforts are being facilitated by groups such as the Internet Alliance that bring together the various members of industry and create a shared collective of experience. There is much that industry can and should teach law enforcement officials about Internet technology, the types of crimes being committed, and the recommended ways in which they might be addressed. However, as we discuss, industry should not, nor does it want to be forced to become the police itself. Here, we try to distinguish the proper roles for government and industry. We propose that industry be cooperative and proactive in assisting law enforcement. It should also define standards, and offer new initiatives in its effort to fight cybercrime, while law enforcement remains under the domain of government. Industry cooperation with law enforcement should be both voluntary and within the limits

of current law. Also in this section, we examine how non-governmental and international organizations may also take active roles in Internet law enforcement and security.

In evaluating the need for cooperation and coordination between and within industry and government, we turn to some specific criminal cases the demonstrate both its successful and unsuccessful applications. We also make some recommendations including the establishment of forums and the sharing of best practices and training methods that may serve to enhance this cooperation and coordination.

As it is with any crime, education is the key to prevention. This requires educating consumers as well as those in government and industry. We assess what is being done and make recommendations for what should be done in utilizing the tools, both technological and human, to teach and train these groups.

Recognizing the international breadth of the Internet as it cuts across borders, cultures and different forms of government, the goal of this paper is to lay the necessary foundation for future discussion. In defining key concepts such as the cooperation between industry and government, we seek to establish a context from which future Internet law enforcement and security initiatives can begin. It is our hope that this paper will achieve its goal in helping to ensure the Internet's success in meeting the many promises of the information age, as we all can use this new medium with confidence and trust.

## THE NATURE AND SCOPE OF THE PROBLEM

Computers can play three roles in criminal activity. First, computers can be targets of an offense. Common examples of this include hacking to steal information or attack Web sites as occurs in denial of service attacks as well as the propagation of computer viruses. Second, computers can simply be the medium in which an offense is committed. This includes the transmission of child pornography, software piracy, Internet identity theft and fraud. Finally, computers can be incidental to a crime. In this case, they may be used to store information or provide other evidence of a crime that has been committed. Of course, these uses for computers (and the Internet) are not mutually exclusive and can all be exploited in the process of committing one crime.[2]

The Internet crime rate is increasing in pace with Internet's explosive growth. Internet users in the US alone are expected to increase from over 100 million in 1999 to 177 million by the end of 2003. Worldwide, the number of users is estimated to reach 502 million by 2003.[3] The economic stakes are also increasing, as e-commerce now accounts for $20 billion of the retail market and is expected to reach $185 billion by 2004. Even more dramatically, business-to-business e-commerce which totaled over $100 billion in 1999 is projected to reach over $2.7 trillion by that time.[4] Without effective law enforcement and security, Internet crime threatens to derail this economic train by creating a loss of consumer and industry confidence in what remains a relatively new medium. Moreover, untold social benefits from Internet-based applications in fields such as medicine, and education may go unrealized without the establishment of trust in online communications.

With such high stakes and high profile events like the recent distributed denial of service attacks on some of the Internet's most heavily trafficked Web sites, some are pushing for a legislative solution. Following the DDoS attacks, a US Senate Hearing on Cybercrime was held to discuss possible actions. The Internet Alliance was called to testify. Some legislators had proposed an immediate increase of penalties for hacking and giving judges more power in authorizing law enforcement's use of tracking technology. In addition, the Federal Bureau of Investigations has been promoting its Cyberspace Security Act (CESA), which would expand the Bureau's powers in fighting cybercrime. Others such as the National Infrastructure Protection Center in the US are also calling for the drafting of new laws to enhance investigative and prosecutorial powers.[5] Not surprisingly, these responses have drawn the ire of civil liberty groups who feel that such action would be an encroachment upon the future of electronic privacy and free speech. We return to this debate later in the paper. However, as we stated before the US Senate, it is our contention that Internet crime is largely an extension of traditional crime and, therefore, can best be addressed through better application of existing law.

## FROM LOCAL POLICE TO INTERNATIONAL ORGANIZATIONS: THE IMPORTANCE OF COORPORATION AND COORDINATION

The international nature of the Internet is obvious. It does not respect geographical boundaries or jurisdictions from country to country. At first glance, it would seem a haven for criminals. Whether it be from home, office, or even on the road from a portable computer, access to the Internet and its global reach is readily

available. Moreover, unlike the Internet, law enforcement agencies must contend with very definite borders and jurisdictional limits. In addition to issues of sovereignty, these agencies must deal with differences among legal systems and a great disparity in technical expertise among their international counterparts. Finally, the nature of the Internet technology helps ensure that most people can use the Internet anonymously. For example, a single transmission may be carried through various Internet Service Providers (ISPs), and from country to country over different media by means of cable, satellite, or wireless technologies. While most Internet users may prefer not to be identified online, this technology makes international traces to identify and locate a computer criminal quite difficult to accomplish.[6]

Given these conditions, the need for international cooperation and coordination among law enforcement agencies is strong. Below, we will address the international efforts that are currently being conducted not only by governments, but by non-governmental organizations (NGOs) and by other international organizations as well.

INTERNATIONAL EFFORTS

In spite of the wide range of legal and technological differences that separate the many nations connected to the Internet, various international efforts are underway to create a more global approach to fighting cybercrime.

As early as 1994, G–7 leaders were emphasizing the need for international cooperation in the developing global information society. Since then, the G–7 and G–8 have identified a select number of pilot projects with key objectives including the support of an international consensus on common principles governing access to computer networks and applications and their interoperability. Another key objective has been the creation of opportunities for information exchange among nations. At the same time, these projects were not supposed to require the formation of new bureaucracies or institutions, and were to be financed by existing programs.[7] Though not specific to fighting crime on the Internet, the G–8's Information Society Pilot Projects have been a useful step in achieving greater global coordination and cooperation, without which it would be impossible to do successfully.

At the end of April of this year, the 41-nation Council of Europe released a draft version of its "Convention on Cyber-Crime." This will be the first international treaty to address criminal law and the procedural aspects of Internet crime.[8] Its purpose is to help harmonize national legislation in this field and facilitate investigations at all efficient levels of cooperation between authorities of different nations. Among the draft's provisions are calls for coordinated criminalization of computer hacking and hacking devices, illegal interception of data and interference with computer systems, computer-related fraud and forgery. In addition, it prohibits online child pornography, including the possession of such material after downloading, as well as the reproduction and distribution of copyrighted material. The draft will also define online criminal acts and attempt to determine the liability of individual and corporate offenders and set minimum standards for applicable penalties.[9]

While these steps to further improve international cooperation and coordination are welcomed, the legal binding nature of the Treaty is somewhat troubling. Future signatory nations will be obliged to give national authorities the ability to perform searches and seizures of computer data and require subjects to produce data under their control and preserve vulnerable data. They will also be obligated to provide assistance to their foreign counterparts, for example by preserving evidence and locating online subjects. This is likely to wreak havoc on existing legal systems that vary widely on issues such as the right to privacy. Civil libertarians have already responded to the plan, saying that it would violate longstanding privacy rights and grant the government far too much power.[10] Industry participation, including the interception of data transmissions by telecom operators and ISPs may also be required when the final draft of this Treaty is released in December 2000. As we discuss below, such demands on industry run contrary to legal protections and would result in the stifling of Internet growth. Similarly, while legal remedies may, in fact, be required to update outdated laws that cannot be applied to new forms of Internet crime, excessive international requirements for new legislation in member countries should be avoided. What is preferred is a voluntary solution by which sovereignty is respected, national and legal values are preserved and mutual assistance is supported.

In January 1999, based on a proposal of the EC, the European Parliament and the Council of the European Union adopted a Multiannual Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. This plan was designed to provide a financial framework for the various EU initiatives on how to deal with undesirable content on the Internet. Its main objectives are to promote industry cooperation and to ensure that this approach is coordi-

nated across Europe and with the rest of the world. In particular, the Action Plan supports four main activities:

- The creation of a safe environment, specifically by setting up a European network of hotlines and encouraging self-regulation and codes of conduct;
- The development of filtering and rating systems, by demonstrating their benefits and facilitating international agreements on rating systems;
- The encouragement of full-scale awareness actions;
- The support of actions, such as assessing legal implications, coordination with similar international activities and evaluating the impact of Community measures.

With a budget of 1 million Euros, contracts for the first three activities have already begun.[11]

Among the various forms of Internet crime, the production and distribution of online child pornography has received especially strong attention from international law enforcement authorities. In 1998, in what was the largest ever Internet raid, over one hundred arrests were made worldwide and nearly one million pornographic images of children were seized. Under the codename "Operation Cathedral," internationally coordinated investigations culminated in simultaneous raids in twelve countries.

The pedophile group targeted in the investigation, the Wonderland Club, was the most sophisticated known to date and operated in secrecy through chat rooms running on discrete servers whose locations were changed on a regular basis. Access was always password protected and supervised. Though the Wonderland Club originated in the US, a breakthrough in the case came when UK police raided a house and seized a computer that contained information about the group. With the help of international bodies like INTERPOL, an agreement was reached by the countries participating in the operation to share key evidence, intelligence and relevant computer data. This was formalized in a Letter of Request and the National Crime Squad in the UK agreed to compile a definitive list of victim images for on-going identification.

The expertise gained from this operation has benefited law enforcement agencies worldwide both operationally and strategically. It has helped in establishing guidelines for computer investigations and in coordinating operational activities. New computer research methods were developed to support established covert policing policies. Combined with the assistance of ISPs, more conventional policing was adopted in order to identify suspects, many of whom used false names, and to gain access to their computer systems and the children who were being abused. Without the application of new technology and international cooperation and coordination, the investigation could not have been successful.[12]

Operation Cathedral's successful methods and procedures should inspire similar efforts in international initiatives to fight other forms of cybercrime. The investigation also highlighted some of the challenges that such endeavors face. The formal Letter of Request system, for example, as a bureaucratic tool, did not provide for fast time exchange of relevant evidence. This demonstrated the more general problem in preparation of cross border evidence. Also, future cross border cooperation may be difficult to achieve when legislative and operational differences between countries can only be overcome through individual determination as opposed to structural and system support.[13]

INTERPOL, in dealing with issues of cybercrime has organized not only a central program at the General Secretariat with an experts working group, but has also promoted and supported regional groups to study issues and solutions particular to their own areas of the world. There may also be value in using the models developed in the hemispheric trade and commerce organizations including NAFTA, APEC, MERCOSUR and CARICOM to study new ways and means for promoting securing security, safety and integrity on the Internet.

## INCLUDING THE LOCAL LEVEL

International efforts alone, however, cannot solve the problem of Internet crime. Although Internet users can transcend geography in the virtual world of cyberspace, their bodies remain in the very real world of their respective local communities. Accordingly, in the case of a burglary or assault, a citizen would likely turn to their local authorities, as the most accessible source for help. In the same way, local authorities should be prepared to assist in the investigation and policing of Internet crime. However, without tying these local efforts to national and international ones, the gaps between could result in overall ineffectiveness. Or worse, this disjointedness could lead to ill-conceived solutions that cause more harm than good.

The importance of inter-jurisdictional cooperation has not gone unnoticed in the United States, for example. In April of this year, the Washington State Attorney

General announced a new initiative that would integrate local, state, and federal efforts in combating cybercrime. The Computer Law Enforcement of Washington (CLEW) cooperative agreement was signed by the US Attorney's Offices in the state of Washington, the FBI, the Washington State Patrol, the Washington Association of Prosecuting Attorneys and Police Chiefs, the State's Association of Sheriffs and the Attorney General's Office. CLEW's focus of bringing together law enforcement from national and local levels to combat Internet crime is one that should be emulated worldwide. Specifically, CLEW is designed to:

- Provide a law enforcement response to high tech crime complaints 24 hours a day, seven days a week;
- Share expertise, resources, and training to help local law enforcement investigate and prosecute Internet crimes;
- Seek funding for a computer forensics lab which is essential for investigating and prosecuting Internet crimes, and;
- Suggest legislation to help prosecute online crime.[14]

The Washington Attorney General's Office also formed a strike team of attorneys and investigators to prosecute consumer protection and criminal cases and to provide expertise to local authorities on Internet crime issues. Another key component of the agreement established the Consumer and Criminal Justice Clearinghouse. With the help of the University of Washington, this Web-based center is designed to educate consumers, parents, teachers, and law enforcement officials about cybercrime issues. In addition, the site will allow for consumers to remove their names from marketing lists and file online complaints.[15]

Other groups in the US have also been created to help inform and educate local law enforcement authorities about Internet and high tech crime. The National Cybercrime Training Partnership's (NCTP) is a training consortium comprised of federal, state, local and international law enforcement agencies and training associations. This group designs, develops and conducts programs to assist investigators and prosecutors of high tech crimes, including those committed on the Internet. With the support of the US Department of Justice and the National White Collar Crime Center, the NCTP has helped local authorities especially to receive training in the latest technologies and methods to address computer-related crime. One example of their efforts is a video that serves as an introduction to the online world and the types of crimes that are committed there. The video also helps local police officers take the appropriate steps in tracking down online criminals and provides information on how to best seize and preserve electronic evidence.[18] The Internet Alliance is also working on a similar video to assist law enforcement officers.

These types of initiatives are particularly useful, as they allow local law enforcement to draw upon the expertise and resources of national and international authorities. While items such as the video may not necessarily give local police all of the specific information they need in helping with an online crime, they can refer them to relevant laws such as the Electronic Communications Privacy Act or to appropriate federal authorities such as the FBI's Computer Analysis Response Team, the US Secret Service and US Customs. These are all useful resources for local police to tap in determining a course of action in investigating or prosecuting an Internet crime.

Other efforts are underway to create interagency alliances within the US federal government. In addition to working with the various consumer and international organizations, the Federal Trade Commission has been active in targeting Internet fraud while working with other agencies from the Securities and Exchange Commission to the Postal Service and the Justice Department.[17]

### AVOIDING CO-REGULATION

It is no surprise that companies in the Internet industry have taken the early lead in confronting cybercrime. For online merchants and other content providers, ISPs, hardware and software companies, it is their very business at stake. These companies are also the technology innovators and have the best understanding of the technical issues with which they work daily. In spite of recent initiatives, governments cannot move at the speed of industry and have been somewhat late in addressing this issue. The Internet Alliance recognizes that law enforcement is trying to catch up with crime in cyberspace and that it needs more resources to do so, or it will seriously fall behind and may never catch up as technology races ahead. At the same time, as a result of their lack of experience and expertise in dealing with the Internet crime, some law enforcement agencies may be tempted to rely upon industry to identify crime, apprehend criminals, and assist in their prosecution.

As in the offline world, this blurring of the line between government and private industry is unacceptable and could have extremely detrimental effects. Members of

the Internet industry should cooperate on a voluntary basis with the proper law enforcement authorities in accordance with existing law. Any new legislation that, in effect, forced industry into being a "co-regulator" with government would stifle innovation and entrepreneurial spirit in this, one of the world's fastest growing sectors. In the end, this could lead to the international flight of companies to countries with more favorable regulatory environments.

Determining the proper role for industry in fighting cybercrime is an international concern. This issue was a key topic at the November 1999 European Commission's Information Society Technologies Conference in Helsinki. In this case, the importance of balanced cooperation between the ISPs and law enforcement was stressed with particular emphasis on having transparent procedures. It was agreed that industry should cooperate only according to the law. There was also consensus that a relationship of mutual respect and trust should be developed between industry and law enforcement authorities.[18]

In explaining the need for the EU's Multiannual Action Plan mentioned above, the European Commission reiterated the need for self-regulation in the Internet industry: "A good cooperation between industry and government might, however, not be sufficient. [The] Internet's technical features, worldwide extension and unlimited accessibility make the application and enforcement of existing rules difficult . . . Existing or new legislation may therefore not be the only or the best tool to fight harmful or illegal content. We therefore need to explore new methods and approaches . . . In developing these approaches, the self-regulatory approach should be the preferred option.[19]

The EC also commented that the July 1999 EC proposal for a Directive on legal aspects of electronic commerce was proposed as an initiative to help eliminate member states' legal differences and divergent approaches to the issue. In particular, it highlighted the proposal's call to establish an exemption from liability for intermediaries where they play a passive role as a "conduit" of information from third parties and limit service providers' liability for other "intermediary" activities such as the storage of information. "A careful balance between the different interests involved is needed, in order to stimulate cooperation between different parties and so reduce the risk of illegal activity online. Once again, industry has a key role to play here by providing for self-regulation, by developing technical solutions and by cooperating with law enforcement agencies."[20]

Such "self-regulation" is desirable as long as it is interpreted as the voluntary cooperation of industry and is not equated with "self-policing." This concept has also been supported by INTERPOL, in its presentation at last year's International Conference on Combating Child Pornography on the Internet. In regards to the responsibilities of ISPs, INTERPOL acknowledged the commitment of ISPs to assist in the detection and elimination of child pornography on the Internet and expressed an understanding of the difficulties ISPs face in controlling what customers distribute through their services. The presentation also included discussion of an initiative that utilized software to centralize, track, and identify cases of child abuse on the Internet. As INTERPOL noted, this project would allow ISPs to support law enforcement in their daily work without having to "police" the Net themselves.[21] Initiatives such as this one that utilize existing technology instead of new regulation or legislation hold promise for easier and faster implementation and, therefore, success. Industry can no doubt accomplish more when motivated by an interest in a marketplace in which consumers have a predictable, positive experience than when it is threatened with civil and criminal sanctions for failing to prevent third-party crimes.

Beginning last year, and spurred by the recent denial-of-service attacks on eight of the Internet's most popular Web sites, the US government has been pushing to make Internet security a top national priority. The initiatives coming from the White House, including an Internet security summit held this February, the Working Group on Unlawful Conduct on the Internet, and a "National Plan for Information Systems Protection," have all called on private industry for help. In response to Clinton's National Plan, subtitled "An Invitation to a Dialogue," which calls for a public-private partnership to assure critical infrastructures, an industry group, the Partnership for Critical Infrastructure Protection, was formed.

Such efforts are useful and productive to the extent that they offer a forum in which information and experience can be shared. However, in the process, the government should avoid overreaction and the "deputizing" of private industry. While it would be fair to say that the Internet industry like all industries has been wary of increased government regulation, this does not mean that private companies wish to assume the roles of law enforcement and prosecutor. Again, the emphasis should be placed on industry's voluntary cooperation and assistance.

INDUSTRY'S SUPPORTING ROLE

While the distinction of the proper roles between law enforcement and the Internet industry must be maintained in combating cybercrime, there are a number of steps that can be taken to make the efforts of both more effective. As the technology leader, industry can offer the government assistance in developing more sophisticated methods to assess Internet crime. Industry should and is contributing to the development of training programs for government agencies. In addition, a directory of appropriate industry and government contacts should be devised to ensure that law enforcement agencies seek assistance from the best resources. In conjunction with the U.S. Department of Justice's recently announced "24/7" computer crime personnel network, the Internet Alliance's Law Enforcement and Security Council is currently developing an online prototype of such a guide. As we discuss below, the LESC is also taking the lead in establishing other initiatives to ensure industry's active support of law enforcement.

Within the Internet industry, a voluntary set of standards or best practices, whether technological, policy-oriented, or other, would aid in the prevention, investigation and prosecution of cybercrime. These standards should respect current business models, allowing flexibility based upon resources that may vary from company to company. For example, while a larger company may be able to establish and support a 24 hour hotline for security and law enforcement contacts, a smaller one may not.

Industry's assistance should also extend to educational efforts including the development and promotion of tools such as parental control software and informative campaigns that help consumers to protect themselves from illegal online activities. Here, the LESC is taking action, not only by promoting the sharing of best practices among its member companies, but also by assisting in the production of these educational materials.

In supporting the government, industry can also work to set up reliable and efficient procedures and channels of communication and cooperation for processing law enforcement requests and passing along investigative material. These efforts can best be achieved through open dialogue within industry and the law enforcement community, facilitated by groups such as the Internet Alliance's Law Enforcement and Security Council. The LESC acts as the primary forum for industry to gather, to assess and to define security problems. This information is also shared among law enforcement agencies, policymakers, and consumers.

In coordination with several agencies, including the Department of Justice and the FBI, the LESC is also preparing updated Internet law enforcement training and resource materials. While many members of the LESC already provide briefings, materials and consultations for the law enforcement community as requested, needs may soon outstrip individual companies' capabilities. By combining an entire industry's experience, efforts such as this one can provide both basic, introductory, and updated, advanced materials to increase law enforcement's expertise and success.[22]

Government can also play a constructive role in enabling and facilitating cooperative industry initiatives, such as statements of good business practices. It can properly use its influence to praise, to critique and to alert consumers to the difference between those companies that are proactive in their efforts and those that are not. However, if such initiatives are to remain viable options for industry, they should not be codified by subsequent legislation. Indeed, for the legislature to take a reasonable, good-faith system of self-regulation and codify it with the imposition of strict duties, inflexible regulations, and the threat of civil and criminal penalties, is a breach of trust that will undermine the willingness of any company to step forward voluntarily in the future.

Initiatives taken by private industry should only complement government efforts and should not replace them. For example, government should first take the time to train its own law enforcement officers in computer and Internet skills irrespective of their jurisdictions. Though many agencies and local authorities may lack experience in dealing with Internet crime, there are some centers of excellence within the Department of Justice, FBI, Attorneys General offices and a few metropolitan police forces. These sources of expertise should be exploited in inter-jurisdictional efforts such as Washington's CLEW program. The LESC also encourages agencies with experience in fighting Internet crime to assist those without it. Within the government, there are also numerous legal authorities to advise on issues of constitutional and statutory civil liberties in the context of the Internet. If given the budgetary resources, law enforcement agencies can also help themselves by hiring additional personnel and supplying them with the proper equipment and materials to investigate and prosecute online crime.

OTHER CASES OF INTERNET CRIME: WHAT CAN BE LEARNED

In October 1998, as part of a worldwide investigation of suspected pornographers, New York State Police seized the computer equipment that local Buffalo, New York ISP, BuffNET, used to provide its subscribers with access to Internet newsgroups. The New York Attorney General said organizers of a virtual college had used the Internet newsgroups to post and trade pornographic images of pre-teens. Thirteen people from four nations were charged in connection with the investigation, but there were no local arrests.

In an issued response, BuffNET stated that it did not create the content under investigation. Nor was it possible for BuffNET, or any ISP, to completely control the postings to its newsgroups. The company did not know about this group or their activity and none of the people charged had BuffNET accounts or uploaded to BuffNET servers. BuffNET received feeds for the newsgroups from other providers including Sprint, Prodigy and a few major educational institutions. In its defense, BuffNET also noted that ISPs are not bound by any state or federal law to moderate their newsgroups. BuffNET even had a history of cooperation with US Customs, the Secret Service, local Sheriffs' offices and the Canadian-American Law Enforcement Organization in tracing the identities of persons involved in illegal Internet activities. The company also has a web page that offers parents information about protecting their children while using the Internet.[23]

Better communication between law enforcement and industry would have helped in this case. Without identifying himself, an undercover investigator from the Attorney General's office e-mailed the company a notification of possible illegal content. BuffNET's attorney reviewed the newsgroup in question and did not find any illegal materials. The Federal Telecommunications Act of 1996 protects service providers from prosecution for materials that are transmitted through their computers, but also obligates them to remove illegal content when they are aware of it.[24] When BuffNET did not remove the site, their equipment was impounded. In this case, which has been likened to the shooting of the messenger, law enforcement authorities could have better coordinated their efforts with members of the ISP industry who were willing to cooperate and provide support in apprehending the true criminals—those who produced and distributed the child pornography.

Law enforcement took a different approach in the case of the Melissa virus. The e-mail spread virus that wreaked havoc on computers worldwide last year was suspected to have been unleashed through on America Online account in the US. AOL was then served with a court order requiring it to turn over information regarding the virus. In addition, the FBI seized a computer of a local Florida ISP which hosted space for the individual suspected of authoring the virus. The FBI also investigated a small ISP in Tennessee through which the virus may have spread. Less than a week after the virus had begun to spread, a third suspect, who later admitted creating it, was arrested in New Jersey.

Indeed, without the help of AOL, the arrest could not have taken place so quickly. According to the New Jersey Attorney General's office, after being served with the court order, the company gave them a tip to the virus' originator, tracking the dissemination source through a listserver.[25]

In this case, industry's best business practices combined with strict compliance with appropriate legal procedures and adherence to principles of due process yielded positive results. Court orders were used when required, privacy was protected and the case was brought to a successful completion. Such protocol will help governments in establishing a good cooperative environment in which industry can assist law enforcement and consumers. Of course, industry also has a vested interest in creating a safer marketplace for its customers. As the owner of the investigated ISP in Tennessee said, "We shut down the Web site . . . We don't like viruses any more than anybody."[26]

In the Melissa case, there was also voluntary assistance from industry, as a software company in Massachusetts proved instrumental in tracing the virus to its authors. In addition, this case revealed the benefits that can come from educational institutions assisting in combating cybercrime, as the Defense Department-sponsored Computer Emergency Response Team at Carnegie Mellon University found digital tracks leading the site where the virus was originally posted. In contrast to the BuffNET case, this investigation proved to be a more positive interaction between government and industry and contributed more toward the cooperative engagement of industry in the future.

As in the Melissa case, the more recent DDoS attacks mentioned above created international concern and sometimes overreaction to an Internet crime. It is important to note that following the report of these attacks on February 7 of this year, Internet services were interrupted for a period of hours, not days. When the assault

was detected, teams of experts deployed additional user capacity and screening tools, quickly bringing the situation under control. This was an impressive demonstration of industry's responsiveness and effective application of technological solutions.

At the same time, the cooperation of industry and law enforcement agencies in this case has already led to the arrest of a Canadian juvenile. Aided by a Canadian Internet Service Provider, the Royal Canadian Mounted Police led a wide-ranging investigation that received input from the FBI, the US Department of Justice and the National Infrastructure Protection Center.

As this paper goes to press, yet another high profile, international virus case is under investigation. In the effort to apprehend the creator of what is being called the "Love Bug" virus, law enforcement agencies from different countries are once again working together and in cooperation with ISPs to solve an Internet crime. In this case, the Love Bug is expected to cause economic damage across the world in excess of $10 billion before its done.[27] As is the Melissa case, industry has been quick to react with technological solutions, as parts of the virus were removed from ISPs' networks and software disinfectants were developed within twenty-four hours of the outbreak.

## PROTECTING PRIVACY WITH EXISTING LAW

Virus cases such as Melissa and the Love Bug have also led to more self-regulatory action by ISP and anti-virus firms. In looking for alternative technological solutions, some ISPs are developing ways to clean their networks so that e-mail is disinfected before it reaches its destination. With technical staff and experience to guide them, some ISPs feel that they can better stay up-to-date with the latest anti-virus software and apply it effectively at the network level. Similarly, many ISPs already provide junk mail filters for their customers. While this may prove a good example of a proactive initiative, not all ISPs are convinced it will work. Scanning incoming e-mail traffic and connecting to billing and directory systems will require significant technical work and expense, they say. Moreover, it may provide a false sense of security and some people might consider it an invasion of privacy.[28] In this way, working within existing laws, the marketplace is determining new ways to fight cybercrime.

Privacy, of course, is a major concern of the Internet industry in its assisting in law enforcement investigations. ISPs and other companies have the utmost concern for maintaining their customers' privacy. At the same, they desire to make their marketplace a safe and secure one and also must comply with the letter of the law.

The first law of its kind, the Electronic Communications Privacy Act was enacted by the US Congress to establish rules and procedures by which law enforcement could have access to an individual's electronic communications and records. These limits on government parallel the approaches traditionally taken in the "bricks and mortar" world. Before information or objects are handed over to law enforcement for investigation, the appropriate warrant, judicial order, or subpoenas must be acquired.

Members of the Internet industry have also developed and implemented policies and internal mechanisms that limit the sharing of personal user information with law enforcement in accordance with the ECPA. This model of industry cooperation and compliance with privacy protection laws could be effectively applied worldwide. However, there are still occasions when law enforcement personnel make investigative requests of companies that fall outside the limits of the law. These requests may also be directed to the wrong persons such as consumer service representatives, rather than others within the ISP structure responsible for handling them. Again, these types of problems can be alleviated through better law enforcement training and communication across the public and private sector lines. In the end, the challenge remains for governments and industry to work together to reach a balance between privacy and law enforcement on the Internet, while taking into account the different laws, structures and norms from society to society.

## EDUCATION: HELPING INTERNET USERS HELP THEMSELVES

Thus far, this paper has focused on law enforcement and industry initiatives to fight Internet crime. However, this solution is incomplete without mention of the role that the Internet's users in the form of consumers, educators, parents and children, should play in helping to help themselves.

Both technological and non-technological tools can help empower the public to minimize risks associated with the Internet and to use the Internet responsibly. Of special importance is how these tools along with relevant knowledge and other re-

sources can be used to guide children's online experience and, in turn, teach them responsible use of the Internet.

Of course, one of the most effective ways of protecting children online is through parents taking a direct role in teaching their children responsible Internet use. Some suggestions include:

- Never give out personal information, such as home address, school name, or telephone number, in a public message such as a chat room or bulletin board;
- Never allow a child to arrange a face-to-face meeting with another computer user without parental permission;
- Get to know your children's online friends just as you get to know all their other friends.[29]

In addition, there are a number of Web sites that give parents guidelines to promote safe and rewarding Internet experiences for children.

Libraries, schools and other public institutions are also developing local solutions to help make cyberspace a safer place for children. Both technological and non-technological, these efforts should be supported by the federal government. Industry should also continue its involvement, as it has through participation in roundtable discussions with government on this issue.[30]

Child protection on the Internet has also gained the attention of non-governmental international organizations. In January 1999, Director General of UNESCO, Federico Mayor hosted a meeting at UNESCO headquarters in Paris to consider ways of combating the exploitation of children on the Net. 300 specialists in childcare and child protection, Internet specialists and service providers, members of the media, law enforcement agencies and other government representatives were in attendance. To implement the resulting action plan and the World Movement of Citizens to Protect Innocence in Danger was created. This group has a small international committee, but the main work is done by National Action Groups and NGOs that enlist the participation of lawyers, Internet specialists, child protection organizations, jurists, political leader and personalities for public relations.[31] Among the Innocence in Danger's achievements thus far, it has helped support regional and international conferences on child pornography on the Internet. It has also produced handbooks for children, parents and teachers, and has created a web-based "electronic watchtower" to provide news and information on the subject. While this program focuses on issues of child pornography it proves a good model for other citizen-based efforts to educate about, and combat, cybercrime.

In assisting law enforcement, some parents are not only teaching their children about online safety, they are also actively seeking out and reporting Internet predators. Thousands of these volunteers are rising up worldwide and their cooperation is welcomed by police, as long as citizens know where to draw the line.[32] Citizens can also contribute directly to law enforcement on the Internet by accessing sites such as the National Center for Missing and Exploited Children's Cyber Tipline www.missingkids.com. The NCMEC has been a key strategic partner for the Internet Alliance since 1996.

Just as they can help in making the Internet safer for children, technological and non-technological tools can be applied in the education of consumers. In the US, the Federal Trade Commission has begun a number of initiatives to educate consumers and give them more confidence in making online transactions. The FTC is also working directly with online marketers and other online entrepreneurs on how to ensure that consumer protection principles apply to their businesses and receives health feedback from these companies that often raises new issues in applying traditional consumer protection to Internet business.

Like the FTC, other US agencies are also working to ensure consumer confidence in the Internet by enforcing legal protections and encouraging private sector leadership. These include initiatives from the Department of Commerce, which has been working with the private sector to develop codes of conduct for business-to-consumer e-commerce and consumer-friendly alternative dispute resolution measures. These measures may prove especially useful in cases hampered by differences in international law. At the request of the FBI, we at the Internet Alliance are working to develop reporting mechanisms for a new Internet Fraud Reporting Center. The Better Business Bureau has also gone online. BBBOnLine is working with industry to help establish guidelines to implement consumer protection. Industry leading ISPs, computer companies, and credit card companies have also formed the Electronic Commerce and Consumer Protection Group. This group works with consumer leaders to develop concrete approaches to address issues of e-commerce confidence.[33]

As with online child pornography, some citizens are doing their own investigative work to combat Internet fraud. Often the victims of fraudulent online auctions, "e-posses" have formed and, in some cases, been able to contribute to the arrest of those committing the offenses. More of these cases will likely wind up on the door-

step of local law enforcement authorities, as one recently did at Suffolk County Police Department in New York.[34] This reemphasizes the need for law enforcement at all levels to have sufficient education, training, and equipment to be able to deal with them effectively.

It is not only police and consumers who can use advice on creating a more secure Internet environment. According to some in the security business, many companies have not taken adequate steps to deal with online attacks. Most companies already have the solution, according to one consultant. "They simply need to do things like avoid shared accounts and blank passwords. Organizations need to understand the risks and prioritize their security [efforts] . . . remembering that most breaches are internal."[35] Others contend that companies alone do not have the resources to effectively prevent network attacks and require managed security monitoring services to provide adequate vigilance.[36] Such debate is healthy and, if pursued in a forum such as the LESC, can lead to the sharing of best practices within industry and greater overall Internet security.

## CONCLUSION

The Internet is still a relatively new medium. Though its sudden and exponential growth over the past ten years has helped to revitalize our economy, its success in the future will require constant dedication and the maintenance of confidence and trust. For this technology to continue to live up to its potential as a positive economic and social force, it must gain the confidence and trust of those who would use it. Internet crime poses an immediate danger to this confidence and trust and therefore, should be a top priority issue for policymakers to address.

There are, as we have seen, many obstacles to effective law enforcement and security on the Internet. In addressing the legal issues associated with this complex technology, we recommend a simple approach. Begin by focusing on the effective enforcement of existing criminal laws. Next, as the Internet Alliance is actively doing, encourage law enforcement to utilize all available resources at all levels of government both domestically and internationally. It is important to realize that the Internet is a simultaneously global and local experience. Accordingly, police efforts must be effective at those levels and all in-between. Otherwise, gaps in law enforcement coverage at one level could lead to overall ineffectiveness.

Government should also learn from industry and vice-versa. This includes training and the sharing of information. It is equally important, however, that the roles of government and industry remain distinct. Industry should be tasked with developing its own leadership and taking a cooperative and proactive role, including the sharing of best practices, the development of technology tools, as well as "cyberethics" curricula and other media to help combat cybercrime. The Internet Alliance and its Law Enforcement and Security Council are working to meet these ends. However, it is also important to remember that actual law enforcement duties should remain the responsibility of appropriate government authorities.

Finally, with the belief that education is the best prevention, both the government and industry should take the time to educate consumers as well as listen to their concerns. Once again, the Internet Alliance is working with industry to promote such educational initiatives. At the same time, consumers should become empowered themselves and seek to do all that they can in the fight against Internet crime.

The Internet has revolutionized modern communication and its greatest chance to live up to its promise will come from the communication and the mutual efforts of government, industry, and consumers. These efforts will be needed to establish confidence and trust in what is still largely a new frontier. It is our intention with this white paper to create a common foundation from which to address the subject of Internet crime and set stage for future discussion.

## ENDNOTES

[1] Andrew Mathews, Building Consumer Trust and Confidence in the Internet Age: An Internet Alliance White Paper, 1999 (Washington, D.C.: Internet Alliance), p. 2

[2] Robert S. Litt, Statement before The Subcommittee on Social Security Senate Ways and Means Committee, United States Senate, May 6, 1997.

[3] United States Dept. of Justice, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet. March 2000, p. 43. *http://www.usdoj.gov/criminal/cybercrime/unlawful.html.*

[4] Robert Lemos, "The Problem: How Big is this Threat?" 2000. ZDNet. 31 March 2000. *http://www.zdnet.com/special/stories/defense/0,10459,2473565,00.html*

[5] Robert Lemos and Lisa M. Bowman, "Overview: Do we Need a 'National Plan?" 2000. ZDNet. 1 May 2000 *http://www.zdnet.com/special/stories/defense/0,10459,2475331,00.html*

[6] United States. Dept. of Justice. Remarks of Deputy Attorney General Eric H. Holder, Jr. at High-Tech Crime Summit in Washington, DC. January 12, 2000. *http://www.cybercrime.gov/dag0112.html.*

[7] National Coordinators: G–8 Global Information Society Pilot Projects, "G–8 Global Information Society Pilot Projects: Interim Report." 1998. Information Society Web Site. 20 April 2000 *http://www.ispo.cec.be/g7/g8interim.html.*

[8] For updates on the treaty, please see the Internet Alliance Web Site. *http://www.internetalliance.org.*

[9] Council of Europe, Draft of Convention on Crime in Cyberspace, April 27, 2000. *http://www.coe.fr/cp/2000/300a(20000).html*

[10] Declan McCullagh, "Cybercrime Solution Has Bugs." 2000. Wired.com. 3 May 2000. http*://www.wired.com/news/print/0,1294,36047.html.*

[11] G.M. Borchardt, Taking Stock: Activities of the European Commission on the Fight Against Child Pornography, 1999 (Austria: European Commission in the Fight Against Child Pornography), p. 2.

[12] Alexander Wood, National Crime Squad: United Kingdom Briefing Note, 1998. (United Kingdom, National Crime Squad).

[13] Wood, National Crime Squad: United Kingdom Briefing Note, 1998. (United Kingdom, National Crime Squad).

[14] Attorney General of Washington, "Law Enforcement Announces Plan to Fight Internet Crime." 2000. *http://www.wa.gov/ago/releases/rel__* internet__042700.html.

[15] Manny Frishberg, "Northwest's Plans vs. Cybercrime." 2000. Wired. 28 April 2000. *http://www.wired.com/news/print/0,1294,35970,00.html.*

[16] The National Cybercrime Training Partnership, Cybercrime Fighting: The Law Enforcement Officer's Guide to Online Crime. Video. United States Dept. of Justice. 1998.

[17] Jeri Clausing, "Interagency Alliances Aim to Fight Cybercrime." 2000. New York Times on the Web. 25 April 2000. *http://www.nytimes.com/library/tech/00/04/cyber/capital/25capital.html.*

[18] Kiveli Ringou, Information Society Technologies Conference 1999: Final Report, 1999 (Helsinki, Finland) p. 22.

[19] Borchardt, Taking Stock: Activities of the European Commission on the Fight Against Child Pornography, 1999 (Austria: European Commission in the Fight Against Child Pornography), p. 2.

[20] Borchardt, Taking Stock: Activities of the European Commission on the Fight Against Child Pornography, 1999 (Austria: European Commission in the Fight Against Child Pornography), p. 2.

[21] ICPO–Interpol General Assembly, Statement to Vienna Interpol Minister. 2000. Vienna, Austria.

[22] Jeff B. Richards, Testimony before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and Judicary. 2000. (Washington, D.C.: Internet Alliance) p. 4–5.

[23] BuffNET, BuffNET's Statement with Respect to Attorney General's Seizure of Internet Equipment. Buffalo News: Nov. 30, 1998.

[24] Editorial, BuffNET Bust: A question of Accountability. Buffalo News: Nov. 9, 1998.

[25] Erich Luening, "Court Papers: Smith admits to creating Melissa Virus." 1999. CNET.com. 3 May 2000. *http://news.cnet.com/category/0–1005–200–346448.html.*

[26] Stephen Shankland, "Melissa Suspect Arrested in New Jersey." 1999. CNET.com. 3 May 2000. *http://news.cnet.com/category/0–1005–200–340689.html*

[27] Morton Overbye, Maria Ressa and Pierre Thomas, "Authorities may be Zeroing in on ILOVEYOU Suspect." 2000. CNN.com. 8 May 2000. *http://www.cnn.com/200/tech/computing/05/05/iloveyou.02.html*

[28] John Borland, "ISP's Look to Kill Viruses Before they Strike" 1999 CNET.Com. December 23, 2000. *http://news.cnet.com/category/0–1004–200–1505088.html*

[29] United States Dept. of Justice, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet. March 2000 *http://www.usdoj.gov/criminal/cybercrime/unlawful.html*

[30] IBID, p. 43.

[31] Homayra Sellier, Innocence in Danger, 1999 (Washington D.C.: World Citizens' Movement to Protect).

[32] Maria Glod, "Mom Hunts Pedophiles on Internet." 2000. Washington Post Online. 13 April 2000 *http://www.newslibrary.com/payoptions/payoption.asp?DBLIST= wp00&DOCNUM=18197&DOCPRICE= 2.95&DOCCURRSYM=$&DOCCURRCODE=usd&ERC=0.*

[33] United States Dept. of Justice, The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet. March 2000, p. 43–49. *http://www.usdoj.gov/criminal/cybercrime/unlawful.html.*

[34] Julia Angwin, "How an E-posse Led to Arrests in Fraud on Online Auction Site" 2000. MSNBC. 4 May 2000 *http://www.msnbc.com/news/403265.asp.*

[35] Robert Lemos and Lisa M. Bowman, "Overview: Do we Need a 'National Plan?" 2000. ZDNet. 1 May 2000 *http://www.zdnet.com/special/ stories/defense/0,10459,2475331,00.html*

[36] Bruce Schneier, "Opinion: The Importance of Vigilance." 2000. ZDNet. 5 April 2000. *http://www.zdnet.com/zdnn/ stories/news/0,4586,2510681,00.html*

Mr. RICHARDS. I saw again that at least among the G-8 members there was a clear belief that law enforcement and security issues are, in fact, shaping the consumer Internet marketplace more than any other factor.

My message today is that, with this committee, the Internet Alliance agrees that law enforcement and security issues are central to achieving consumer confidence and trust. At the same time, we are not enthusiastic about and don't today support proposals to legislate privacy. If time allows, I will touch on why privacy legislation could have unintended consequences, increase tensions over jurisdiction, and most of all distract us from the critical point of agreement here, effective enforcement of current law.

I make these points about best practices and the success that industry has had and government has encouraged us to develop because in the areas of security and privacy we offer the committee an outstanding example of voluntary private sector action and an unusual record of achievement.

Mr. Chairman, in S. 2448 you have proposed ambitious security and privacy legislation, and we express today our appreciation for your sensitivity to a number of industry needs and concerns in its drafting. Among its provisions on the security side are additional powers and resources for law enforcement in the Internet space, increased penalties for existing crimes and the addition of new conduct to the criminal code, and provisions for expanded law enforcement cooperation with computer crime investigations by foreign jurisdictions.

While we approach any legislation governing the Internet with extreme caution, we feel that some of these provisions are of positive interest to industry. By way of background, we have become vigorously involved in building bridges between industry and law enforcement. We last fall launched our Law Enforcement and Security Council as a global initiative, again focused on effective enforcement of current law. And we are today partnering with law enforcement globally, especially with INTERPOL and others, to improve training and coordination. So we are putting our money where our mouth is on these issues.

Now, I have also testified in support of additional budgetary and personnel resources for law enforcement before Senator Gregg's appropriations subcommittee earlier this year. At the same time, we recognize there are times when current law needs to be amended by narrowly tailored legislation, and so we advocate the criminal provisions outlawing false e-mail and message identification information as a key step empowering consumers to reduce the amount of unsolicited e-mail, and to assist ISPs, Internet service providers, to block outgoing messages which may be part of, let's say, a denial

of service attack. We are convinced it is a necessary foundation for other consumer empowerment and law enforcement initiatives.

With respect to other security-related provisions, we favor giving law enforcement adequate tools to investigate and prosecute criminal acts online. However, we do also share the misgivings of some civil liberties groups and others over law enforcement requests to expand wholesale the trap and trace or pen register laws to the Internet context.

While useful to law enforcement, we feel these steps can threaten to undermine consumer confidence and trust, and subject the actions and communications of innocent users to an unparalleled level of Government monitoring and intrusion. At the same time, it could implicate ISPs and Web site hosts to an unprecedented level of participation in criminal investigations and lead to mandatory, impractical data retention requirements. We commend you for having resisted these proposals in the drafting of S. 2448.

In our society, we have never subscribed to the idea that safety and security is worth the sacrifice of all freedoms. We accept some measure of risk, some inefficiency in our criminal law system, because we also attach a high value to individual freedom and privacy from government intrusion. So we feel strongly that the Fourth Amendment and statutory protections such as ECPA must be safeguarded and made applicable to the online context.

As our final security side point, we have long urged greater domestic law enforcement cooperation with foreign law authorities. However, the international character and ease of use of the Internet, as we have seen with recent virus attacks, makes it clear that cross-border crimes will become frankly more common. So we clearly support increased budgetary, personnel, and training resources for those purposes. We think the international dialogue will protect consumers.

In conclusion, getting it right, we believe, is essential. And there is one other specific point from my written statement that I really must note. A key factor from an industry standpoint is preemption of State and local laws. This comes as no surprise. The Internet provides the most compelling scenario in recent memory for uniformity of legal treatment across State and national borders.

Thus, we support your proposal. We think that there are issues about preemption, about the constitutional sense of occupying the field with respect to duties and risks of e-businesses. I want to finally move on and commend you and thank you for the public education aspect of S. 2448. We think it is absolutely crucial.

I stand ready to answer any of your questions, and thank you.

[The prepared statement of Mr. Richards follows:]

PREPARED STATEMENT OF JEFF B. RICHARDS

Good morning, I am Jeff Richards, Executive Director of the Internet Alliance. Since our founding in 1982 as the Videotex Industry Association, the Internet Alliance (IA) has been the only trade association to address online Internet issues from a consumer Internet online company perspective. Through public policy, advocacy, consumer outreach and strategic alliances, the IA is building the trust and confidence necessary for the Internet to become the global mass-market medium of this century. The Internet Alliance's members represent more than ninety percent of consumer access to the Internet in the United States. Since May of 1999, the Internet Alliance has been a separate subsidiary of the Direct Marketing Association,

bringing the resources of a 4,500-member organization to bear on consumer Internet issues and their resolution.

Our mission is to increase consumer trust and confidence in the Internet by promoting good business practices, public education initiatives, enforcement of existing laws protecting consumers, and the development of a legal framework governing the Internet that will provide at the same time predictability and efficiency, security and freedom to innovate.

I am pleased to be able to offer the Alliance's views on Internet security and privacy, and particularly on S. 2448. IA's consumer e-business focus gives its views particular relevance. Among the key issues affecting the willingness of consumers to use the Internet is security, law enforcement, and privacy. For example, while privacy is among the most cherished American values, ironically it is not an absolute proposition, but a flexible and evolving set of expectations. Indeed those expectations change according to individual circumstances, such as where we are, what we are doing, and what stage of life we're in, as well as changing along with our culture and technology. Clearly, analyzing privacy in simplistic terms, while appealing, is unlikely to lead us to an optimal level of consumer satisfaction.

In particular, then, I will focus on security matters. Coming as I did from last week's G8 meeting during which we released the Internet Alliance White Paper entitled "An International Policy Framework for Internet Law Enforcement and Security," I saw again that—at least among the G8 members—there was a clear belief that law enforcement and security issues are in fact shaping the consumer Internet marketplace more than any other. My message today is that, with this Committee, the Internet Alliance agrees that law enforcement and security issues are central to achieving consumer confidence and trust. At the same time, we are not enthusiastic about and do not today support proposals to legislate privacy. For reasons that we will touch on later, privacy legislation invites unintended consequences, increases tensions over jurisdiction, and distracts us all from the critical point of agreement—effective enforcement of current law.

IA members recognized several years ago, in the infancy of e-commerce, the importance of consumer confidence and trust in the protection of their data, and they were instrumental in designing the first privacy "best practices" guidelines. Beginning with our creation of the first industry privacy principles in 1996, and continuing through initiatives like TRUSTe, BBBOnline, and the Online Privacy Alliance's privacy guidelines, as the Internet was commercialized the private sector has changed the e-commerce landscape in favor of the consumer. At the same time government has monitored these efforts but has expressly endorsed industry leadership and encouraged corporate participation in these voluntary efforts, while forbearing to legislate. This approach to Internet regulation has proven very constructive.

I make these points because the areas of security and privacy of personally identifiable information offer the Committee an outstanding example of voluntary private sector action resulting in an unusual record of achievement. As noted in recent studies, over 90 percent of recently surveyed commercial web sites post privacy policies, a huge advance over the last two years; and the quality of the disclosures and other features is also rapidly increasing. It is doubtful that either government or non-profit sites come close to this level of performance. Most importantly, there is no question that industry has brought these benefits to consumers more rapidly than could have been the case under the compulsion of formal federal regulations. Likewise, the inherent flexibility of business-led efforts has allowed for a more prompt and tailored response to subsequent challenges, such as those posed recently by the evolution of ad server practices, that government has helped highlight.

This provides evidence that the optimal approach to consumer Internet issues is almost always found in a combination of efforts, a three-way partnership among industry committed to better serving customers, government committed to effectively enforcing current law, and an empowered public knowledgeable of its choices and competent to decide for itself among a range of options. I stress that as it addresses the rapidly changing Internet, government has a useful, even essential role. However, that role should rarely lead it to impose new legislative mandates and constraints, and then only by the least restrictive means available.

These ideas form the framework for the rest of my comments. We commend the Committee for its leadership role in oversight of the Internet and the many issues raised as the new medium alters our economy and our society in significant ways. The context for this hearing is compelling: just over the last few months, public attention has been focused on large-scale distributed-denial-of-service attacks, hacking of sensitive databases, a new set of viruses, and this week, the release of the Federal Trade Commission's annual e-commerce site privacy survey and recommendations. These are the kinds of events that normally generate widespread support for responsive legislation. We must keep in mind, however, that in each case the re-

sponse of industry and, where laws were broken, law enforcement, has been quick and effective. This was without new laws or expanded enforcement authorities.

Mr. Chairman, Mr. Schumer, in S. 2448 you have proposed ambitious security and privacy legislation; and we express our appreciation for your sensitivity to a number of industry needs and concerns in its drafting. It covers several general areas: on the security side, 1) additional powers and resources for law enforcement in the Internet space; 2) increased penalties for existing crimes and the addition of new conduct to the criminal code; and 3) provisions for expanded law enforcement cooperation with computer crime investigations by foreign jurisdictions. On the privacy side: requirements that e-businesses give consumers notice before collection of personally identifiable information, and choice over how that information, if collected, can be disclosed to others. You have asked for our reaction to these initiatives.

While we approach any legislation governing the Internet with extreme caution, we feel that S. 2448 does contain security-related provisions of positive interest to industry. By way of background we have become vigorously involved in building bridges between industry and the law enforcement community. Last fall the Internet Alliance launched the Law Enforcement and Security Council as a global initiative focused on the effective enforcement of current laws. The LESC is partnering with several law enforcement agencies to improve training and coordination in the enforcement of existing laws. We feel additional budgetary and personnel resources for these agencies, and more widespread training of and coordination among investigative and prosecutorial officers, to be the steps that would provide maximum benefit to all who use the Internet. I myself testified in support of these resources before Sen. Gregg's Appropriations Subcommittee earlier this year. Again, we feel increased enforcement of current laws is almost always sufficient to protect the public.

At the same time, the Internet Alliance also recognizes there are times when current law needs to be amended by narrowly tailored legislation in order to enhance effective enforcement. Thus, we advocate criminal provisions outlawing false email and message identification information, as a key step in empowering consumers to reduce the amount of unsolicited email, and in assisting ISP's to block outgoing messages which may be part of a distributed denial of service attack. We appreciate your inclusion in S. 2448 of a provision directed to these concerns. While it is not a complete solution in itself, we are convinced it is a necessary foundation for other consumer empowerment and law enforcement initiatives, some of which have been proposed in other bills.

With respect to the other security related provisions, the IA favors giving law enforcement adequate tools to investigate and prosecute criminal acts online. Our enforcement agencies are instrumental in contributing to the high quality of life we enjoy in America. As the Internet has emerged, they have been called on to meet extraordinary new challenges. In general, they are doing a fine job, as demonstrated by their successes in responding to the recently publicized DDoS, hacking and virus attacks, but there are modest changes in law which would further improve their ability to protect the public. We support S. 2448's proposals to satisfy the $5,000 threshold on computer crimes by expanding the definition of and allowing the aggregation of damages, and to give nationwide effect to certain evidentiary court orders. Experience has shown that current rules in these areas fall short in real world application.

However, we share the misgivings of civil liberties groups and others over law enforcement requests to expand wholesale the scope of trap and trace or pen register laws in the Internet context. While useful to law enforcement, we feel these steps threaten to undermine consumer confidence in the Internet and subject the actions and communications of innocent users to an unparalleled level of government monitoring and intrusion. At the same time, they could implicate ISP's and web site hosts in an unprecedented level of participation in criminal investigations and lead to mandatory, and impractical, data retention requirements. We commend you for having resisted these proposals in drafting S. 2448.

In our society, we have never subscribed to the idea that safety and security is worth the sacrifice of all freedoms. We accept some measure of risk, some inefficiency in our criminal law system, because we attach such a high value to individual freedom and privacy from government intrusion. Thus, the Internet Alliance feels strongly that Fourth Amendment and statutory protections such as ECPA must be safeguarded and made applicable in all online contexts. It is not reasonable to believe Internet users are greatly concerned about corporate use of personally identifiable information, but that they have little interest in government access to the same data. Survey results consistently have shown the opposite.

We also would like to raise concerns about the impact of broadening the scope of criminal conduct for computer crimes, and about the effect of the new hacking provi-

sions. We concur with the addition of computer crimes to the list of offenses for which wiretaps may be sought. On the other hand, I believe you would agree that the federal role in law enforcement is a special one, and as we think about expanding our ability to combat hacking by broadening proscribed conduct, we should avoid spreading the net so far as to encompass relatively harmless nuisances and pranks. In addition, our members feel strongly that any hacking provisions must not compromise their ability to hack into their own systems, or to hire others to do so. This is a technique essential to the ongoing process of discovering system weaknesses and correcting them. We have not concluded that the language of S. 2448 poses these problems, but we would like to work with you to make sure the right balance is clearly struck.

On our final security-side point, we have long urged greater domestic law enforcement cooperation with foreign criminal law authorities. Positive examples can be found, such as the assistance both the consumer Internet industry and U.S. law enforcement officials gave in the Philippine investigation of the "Love Bug" virus. However, the international character and ease of use of the Internet makes it inevitable that cross-border crimes will become more and more common. Again, we support increased budgetary, personnel and training resources for this purpose. And we have no substantive concerns with many of the international cooperation provisions of S. 2448. We offer the following examples as starting points for effective international dialog:

- The law as finally amended should not require businesses to change their business practices to accommodate the needs of foreign, or domestic, criminal investigations.
- The law should not impose significant, uncompensated expenses on ISP's or other e-businesses in responding to requests by law enforcement at the behest of foreign authorities.
- It should not require business involvement in the investigation of conduct which is constitutionally protected in the United States or which is consistent with our underlying values. We believe S. 2448 contains language designed to produce this result, though we would like to review the specific wording with you to make sure it's effective.
- Immunity from suit should be extended to those who in good faith comply with investigative requests under the law, which are valid on their face.

Turning now to privacy, I would like to make a few general comments. It is clear that privacy is growing as a federal legislative issue. Some policymakers and the media, in particular, are coming to believe that they grasp the complexity of the issue and the options available, and that the time has come for a decision on what federal privacy legislation should look like. As I noted at the beginning of my testimony, industry has always been at the forefront of thought, discussion and action in improving privacy protections available to Internet users. Yet, we in the business community are acutely aware that because of the complexity of cause-and-effect in the Internet space, even well intentioned legislation developed after several years of experience poses both to business and to consumers significant risks of unintended consequences. Hence, we must be involved in providing you the best of our knowledge and expertise.

From our standpoint, "getting it right" is essential:

- Technology and business models are changing quickly, and require policymakers to acquire current factual knowledge and develop insight into future trends, so as not to rob consumers of new Internet functions or capabilities—and prevent new privacy innovations and solutions.
- Policy models to date have rested on assumption about what consumers want. There is a growing body of data indicating that they vary widely in their desires and expectations. We would all benefit from increased knowledge in this area.
- Industry's voluntary response to the privacy challenge has been remarkably successful in delivering real benefits to consumers, and it is increasingly effective. We must be careful not to sap this momentum.
- Quite significantly, it is becoming clear that we will not legislate in a vacuum. Other nations have taken up the privacy issue and still others may do so. As an example, it has taken the U.S. and the European union two strenuous years to negotiate "safe harbor" rules, which have yet to be tested in practice. In the United States, for example, we have looked at issues in a sector-by-sector approach, such as children, or the financial sector. In Europe, by contrast, there has been a more general approach.
- These are complicated issues. We must take the time to integrate an international view into our thinking and assure ourselves that whatever we do will serve us both domestically and internationally.

A key factor from an industry standpoint is pre-emption of state and local laws. This comes as no surprise: the Internet provides the most compelling scenario in recent memory for uniformity of legal treatment across state, and indeed, national, borders. It is clear that S. 2448 does not contain the kind of language which in a constitutional sense "occupies the field" with respect to duties and risks of e-businesses in collecting and disseminating personally identifiable information.

In short, the privacy issue has been joined on many levels. I can assure you that we are every bit as committed as you are to giving consumers a secure and satisfying online experience. We hope to work with you to increase your knowledge of the complex dynamics at work here, dynamics just as subtle and involved as those in the areas of financial and medical privacy.

Finally, let me commend you on the public education campaign called for in S. 2448. We have consistently said that consumer empowerment is the essential ingredient in a successful national privacy policy, and education is a vital component of empowerment. Thus, we support your proposal, but we'd like to help improve it.

To a significant degree, the current debate on privacy is distorted by the perception that the sharing of personal information benefits only the corporate recipient. This of course is incorrect. While the public, and many of us, have come to see the Internet as "free," even on the Internet, free lunches are few and far between. It costs website hosts, merchants, ISP's and other significant resources to create and handle the traffic for useful, attractive, entertaining experiences for consumers. Even for large sales-oriented sites, these are not small components of the cost of doing business. But for most, access to information from consumers who make purchases, or who just visit, is critical to support revenue from web site advertisers.

The Internet offers new opportunities for data sharing and for consumer benefit. Moreover, its ability to save consumers time on purchases and to more perfectly match their expectations on variety, price, performance and other factors is unrivaled in the bricks and mortar world. Yet, because the Internet is an interactive medium, its advantages of speed and satisfaction are directly dependent on the sharing of information. These benefits will only increase in the future as the technology matures.

Thus, we recommend that the public education campaign communicate a balanced view of the risks and benefits to sharing information. We'd be glad to consult with you on this task.

Again, Mr. Chairman, Sen. Schumer, members of the committee, we appreciate the opportunity to comment on these important issues, and we look forward to an ongoing and constructive dialogue. I'd be glad to answer any questions.

The CHAIRMAN. Thank you, Mr. Richards.

Mr. Dempsey, we will take your testimony now.

## STATEMENT OF JAMES X. DEMPSEY

Mr. DEMPSEY. Good morning, Mr. Chairman. Senator Feinstein, good morning. Thank you, Mr. Chairman, for inviting us to testify at this important hearing on the issue of Internet security and privacy. We congratulate you on your leadership and foresight in beginning to grapple with these difficult issues both from the law enforcement perspective and from the consumer perspective.

The Center for Democracy and Technology is an Internet privacy and civil liberties organization, and we come here today with three main points. Law enforcement obviously must have sufficient authority to fight crime online. In your bill, 2448, section 109 and section 402 of that bill, you have some important provisions increasing the resources for law enforcement. They obviously need to build up their expertise to be able to deal with this new kind of crime.

But at the same time, we must recognize that it is the Internet industry, the designers and builders of this technology, of this amazing new network, this amazing new communications medium—it is the people who run it and operate it and run the critical infrastructures who are really in the best position to prevent hacking crimes and to protect the critical infrastructure by building more secure products and networks.

And it is clear that industry, after probably not giving security the priority that it deserves, is now focusing on this issue a tremendous amount of resources cooperatively, and that is far more likely to solve this problem than government intervention.

Second, given the tremendous increase in surveillance powers brought about by the new technology, we must avoid any expansions of government surveillance authority, and instead focus on the privacy standards and strengthen the privacy controls governing government monitoring of communications and access to stored records. I will discuss in a minute some of the ways in which the current privacy standards for government surveillance and government data collection have not kept pace with the change of this technology.

Third, for consumer privacy, we must seek a solution that is suited to the rapidly changing nature of the Internet, and the ultimate solution will combine both the privacy-enhancing potential of the technology itself—we need to actually use this technology to improve privacy, not to merely erode privacy—and, secondly, self-regulation driven by consumer demand. Consumers want privacy, and industry is hearing that and beginning to address those consumer concerns. And ultimately, as your legislation recognizes, we will need Federal baseline standards that are enforceable against the bad actors and the outliers to protect consumers and their privacy online.

I wanted to focus primarily on some of the Fourth Amendment issues, where this committee, along with the rest of society, is confronted with what might seem like a dilemma: how do we address crime online without intruding on privacy.

I think that there are two observations here. One is that the Internet is a unique, decentralized, user-controlled medium. And far more than with any other type of crime, the solutions to hacking, the solutions to Internet crime and attacks lie in the hands of industry and the people who use this technology. Obviously, as you said in your opening statement, that is where our first emphasis has to be.

And the role of the Government is always going to be, of necessity, I think, limited, and the ability of the Government is going to be limited to bring about improvements in the private sector. The Government has enough to do to get its own house in order.

Second, it is clear if you look at the broad sweep of technology that the powers of law enforcement to collect information, the access to information, has dramatically increased. Yet, the last time we updated our privacy laws governing criminal investigations was in 1986 with ECPA, the Electronic Communications Privacy Act, which came out of this committee.

Think of all the changes that have occurred since 1986 and the vast amount of information that is now available online. We need to develop privacy standards that address that. The Justice Department is pushing for an expansion in authority, particularly in terms of the pen register. And there is some merit, I think, to their claim of need for a nationwide pen register order.

But by the same token, if you look at that underlying statute, the standard in that statute is the rubber stamp standard. There is no authority of the judge to review that Government application. So

before we extend that authority to the Internet, before we make it nationwide in effect and give this sort of roving authority, we need to go back, look at the basic standards in the Title 18 investigatory provisions, and increase those standards to put some real teeth in it, to give the public the kind of Fourth Amendment privacy protections that they expect in the offline world to begin extending those more fully to the online world.

We are prepared to work with you, Mr. Chairman. We coordinate the Digital Privacy and Security Working Group, which is a group of industry and public interest organizations, and we will make that forum available to you and your staff and to the other members of the committee to begin to try to build some consensus and develop a narrowly focused bill. We can't allow this, I think, to become a Christmas tree.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Hatch, we thank you and Senator Leahy for the opportunity to testify today on the important issue of internet security and privacy. We congratulate both of you, and Senator Schumer, for your leadership and foresight in beginning to grapple with these difficult issues, both from the law enforcement perspective and from the consumer privacy perspective. S. 2448 and the other introduced bills have served to launch an important dialogue. Consensus has not been achieved yet, and we share with you today some of our concerns about various proposals that are being put forth, but CDT is committed to working with you, Mr. Chairman, and other members of this Committee, to develop narrowly focused and properly balanced legislation.

The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic values on the Internet. Our core goals include ensuring that the Constitution's protections extend to the Internet and other digital information technologies, and that public policies and technical solutions provide individuals with control over their personal information online. CDT also coordinates the Digital Privacy and Security Working Group (DPSWG), a forum for more than 50 computer, communications, and public interest organizations, companies and associations working on information privacy and security issues.

Our main points today are three-fold:

• While law enforcement must have sufficient authority to fight crime in cyberspace, we must recognize that the Internet industry is in the best position to prevent hacking crimes and protect critical infrastructures by building more secure products and networks.

• Given the tremendous increase in surveillance power brought about by the new technology, we must avoid expansions of government surveillance authority and instead must strengthen the weak and outdated privacy standards controlling government monitoring of communications and access to stored records.

• For consumer privacy, we must seek a solution suited to the rapidly changing Internet, combining the privacy-enhancing potential of the technology itself, self-regulation driven by consumer demands for privacy, and federal legislation that sets baseline standards and provides remedies against the bad actors and outliners.

We focus in this testimony primarily on the Fourth amendment issues, where this Committee, along with the rest of society, is confronted with what might seem to be a dilemma: how to fight crime on the Internet without intruding on privacy.

A starting point in resolving this apparent dilemma is to recognize that the Internet is a uniquely decentralized, user-controlled medium. Hacking, unauthorized access to computers, denial of service attacks, and the theft, alteration or destruction of data are all already federal crimes, and appropriately so. But Internet security is not a problem primarily within the control of the federal government. Particularly, it is not a problem to be solved through the criminal justice system. Internet security is primarily a matter most effectively addressed by the private sector, which has built this amazing medium in such a short time without government interference. It is clear that the private sector is stepping up its security efforts, with an effectiveness that the government could never match, given the rapid pace of

technology change and the decentralized nature of the medium. The tools for warning, diagnosing, preventing and even investigating infrastructure attacks through computer networks are uniquely in the hands of the private sector. In these ways, Internet crime is quite different from other forms of crime. While the potential for the government to help is limited, the risk of government doing harm through design mandates or further intrusions on privacy is very high.

Second, while the Justice Department frequently complains that digital technologies pose new challenges to law enforcement, it is clear, if you look at the Justice Department's record, that the digital revolution has been a boon to government surveillance and collection of information. In testimony on February 16, 2000 before the Senate appropriations subcommittee, FBI Director Freeh outlined the Bureau's success in many computer crime cases. Online surveillance and tracking led to the arrest of the Phonemasters who stole calling card numbers; the Solar Sunrise culprits, several of whom were located in Israel; an intruder on NASA computers, who was arrested and convicted in Canada; the thieves who manipulated Citibank's computers and who were arrested with cooperation of Russian authorities; Julio Cesar Ardita, who was tracked electronically to Argentina; and the creator of the Melissa virus, among others. Computer files are a rich source of stored evidence: in a single investigation last year, the FBI seized enough computer data to nearly fill the Library of Congress twice. Electronic surveillance is going up, not down, in the face of new technologies. The FBI estimates that over the next decade, given planned improvements in the digital collection and analysis of communications, the number of wiretaps will increase 300 per cent. Last year, the largest rate of increase in government intercepts under Title III involved newer electronic technologies, such as email, fax and wireless devices. Online service providers, Internet portals and Web sites are facing a deluge of government subpoenas for records about online activities of their customers. Everywhere we go on the Internet we leave digital fingerprints, which can be tracked by marketers and government agencies alike. The FBI in its budget request for FY 2001 seeks additional funds to "data mine" these public and private sources of digital information for their intelligence value.

Considering the broad sweep of the digital revolution, it is apparent that the major problem now is not that technology is outpacing government's ability to investigate crime, but, to the contrary, that changes in communications and computer technology have outpaced the privacy protections in our laws. Technology is making ever-increasing amounts of information available to government under minimal standards falling far short of Fourth Amendment protections.

Nonetheless, the Justice Department is seeking further expansions in its surveillance authorities. But surely, before enacting any enhancements to government power, we should ensure that current laws adequately protect privacy. For example, the government wants to extend the pen register statute to the Internet and create a "roving" pen register authority. Yet, the current standard for pen registers imposes no effective control on the government, reducing judges to mere rubberstamps. And pen register as applied to Internet communications are even more revealing. In this and other cases, we must tighten the standards for government surveillance and access to information, thus restoring a balance between government surveillance and personal privacy and building user trust and confidence in these economically vital new media. CDT is prepared to work with the Committee and the Justice Department to flesh out the needed privacy enhancements and to convene our DPSWG working group as a forum for building consensus.

BACKGROUND: FOURTH AMENDMENT PRIVACY PRINCIPLES

To understand how far current privacy protections diverge from the principles of the Constitution, we should start with the protections accorded by the Fourth Amendment. If the government wants access to your papers or effects in your home or office, it has to meet a high standard:

- The government must obtain a warrant from a judge based on a showing of probable cause to believe that a crime has been, is being or is about to be committed and that the search will uncover evidence of the crime. The warrant must "particularly" describe the place to be searched and the things to be seized.
- The government must provide you with contemporaneous notice of the search and an inventory of items taken. See *Richards* v. *Wisconsin,* 520 U.S. 385 (1997); *Wilson* v. *Arkansas,* 514 U.S. 927 (1995).

These rules apply in the computer age, so long as you keep information stored on your hard drive or disks in your home or office.

The Supreme Court held in 1967 that wiretapping is a search and seizure and that telephone conversations are entitled to protection under the Fourth Amendment. *Katz* v. *United States, 389 U.S. 347 (1967), Berger* v. *New York,* 388 U.S. 41

(1967). Congress responded by adopting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, requiring a court order based on a finding of probable cause to intercept wire or oral (i.e., face-to-face) communications. 18 U.S.C. § 2510 et seq. However, Congress did not require the contemporaneous notice normally accorded at the time of a search and seizure. This was a fateful decision, but, the government argued, to give contemporaneous notice would defeat the effectiveness of the surveillance technique. In part to make up for the absence of notice, and recognizing the other uniquely intrusive aspects of wiretapping, Congress added to Title III requirements that go beyond the protections of the Fourth Amendment. These additional protections included: permitting the use of wiretaps only for investigations of a short list of very serious crimes; requiring high-level Justice Department approval before court authorization can be sought; requiring law enforcement agencies to exhaust other, less intrusive techniques before turning to eavesdropping; directing them to minimize the interception of innocent conversations; providing for periodic judicial oversight of the progress of a wiretap; establishing a statutory suppression rule; and requiring detailed annual reports to be published on the number and nature of wiretaps.[1]

After it ruled that there was an expectation of privacy in communications, the Supreme Court took a step that had serious adverse consequences for privacy: It held that personal information given to a third party loses its Fourth Amendment protection. This rule was stated first in a case involving bank records, *United States* v. *Miller*, 425 U.S. 435 (1976), but it is wide-ranging and now serves as the basis for government access to all of the records that together constitute a profile of our lives, both online and offline: credit, medical, purchasing, travel, car rental, etc. In the absence of a specific statute, these records are available to law enforcement for the asking and can be compelled with a mere subpoena issued without meaningful judicial control.

In 1979, a third piece of the privacy scheme was put in place when the Supreme Court held that there is no constitutionally-protected privacy interest in the numbers one dials to initiate a telephone call—data collected under a device known as a "pen register." *Smith* v. *Maryland*, 442 U.S. 735, 742 (1979). While the Court was careful to limit the scope of its decision, and emphasized subsequently that pen registers collect only a very narrow range of information, the view has grown up that transactional data concerning communications is not constitutionally protected. Yet, in an increasingly connected world, a recording of every telephone number dialed and the source of every call received can provide a very complete picture—a profile—of a person's associations, habits, contacts, interests and activities. (Extending this to email and other electronic communications can, as we explain, below, be even more revealing.)

In 1986, as cellular telephones service became available and email and other computer-to-computer communications were developing, this Committee recognized that the privacy law was woefully out of date. Title III anachronistically protected only wire and voice communications: it did not clearly cover wireless phone conservations or email. In response, under the leadership of Senator Leahy, Congress adopted the Electronic Communications Privacy Act of 1986 (ECPA). ECPA did several things: it made it clear that wireless voice communications were covered to the same degree as wireline voice communications. It extended some, but not all, of Title III's privacy protections to electronic communications intercepted in real-time.

ECPA also set standards for access to stored email and other electronic communications and transactional records (subscriber identifying information, logs, toll records). 18 USC § 2701 et seq. And it adopted the pen register and trap and trace statute, 18 USC § 3121 et seq., governing real-time interception of "the numbers dialed or otherwise transmitted on a telephone line." (A pen register collects the "electronic or other impulses" that identify "the numbers dialed" for outgoing calls and a trap and trace device collects "the originating number" for incoming calls.) To obtain such an order, the government need merely certify that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 USC

[1] Over time, though, many of these additional protections have been substantially watered down. The list of crimes has been expanded, from the initial 26 to nearly 100 today and more are added every Congress. Minimization is rarely enforced by the courts. The exhaustion requirement has been weakened. Evidence is rarely excluded for violations of the statute. Almost every year the number of wiretaps goes up—12% in 1998 alone. Judicial denials are rare—only 3 in the last 10 years. The average duration of wiretaps has doubled since 1988. So even in the world of plain old telephone service we have seen an erosion of privacy protections. The fragility of these standards is even more disconcerting when paired with the FBI's "Digital Storm" plans for digital collection, voice recognition and key word searching, which will reduce if not eliminate the practical constraints that have up to now limited the volume of information that the government can intercept.

§§ 3122–23. (There is no constitutional or statutory threshold for opening a criminal investigation.) The law states that the judge "shall" approve any request signed by a prosecutor.

ECPA did not, however, extend full Title III protections to email sitting on the server of an ISP. Instead, it set up a two-tiered rule: email in "electronic storage" with a service provider for 180 days or less may be obtained only pursuant to a search warrant, which requires a finding of probable cause, but the additional protections of Title III—limited number of crimes, high level approval, judicial supervision—do not apply. Email in storage for more than 180 days and data stored on a "remote computing service" may be obtained with a warrant or a mere subpoena. In no case is the user entitled to contemporaneous notice. The email portions of ECPA also do not include a statutory suppression rule for government violations and do not require annual reports of how often and under what government access, which are critical for public or congressional oversight.

MAPPING THE FOURTH AMENDMENT ONTO CYBERSPACE

Remarkably, ECPA was the last significant update to the privacy standards of the electronic surveillance laws. Astonishing and unanticipated changes have occurred since 1986:

- the development of the Internet and the World Wide Web as mass media;
- the convergence of voice, data, video, and fax over wire, cable and wireless systems;
- the proliferation of service providers in a decentralized, competitive communications market;
- the movement of information out of people's homes or offices and onto networks controlled by third parties;
- the increasing power of hand-held computers and other mobile devices that access the Internet and data stored on networks.

As a result of these changes, personal data is moving out of the desk drawer and off of the desktop computer and out onto the Internet. Unless Congress responds, the Fourth Amendment protections would remain available only in the home when increasingly information is not stored there anymore. It is time to adopt legislative protections that map Fourth Amendment principles onto the new technology.

It is clear that the surveillance laws' privacy protections are too weak:

- Data stored on networks is not afforded full privacy protection. Once something is stored on a server, it can be accessed by the government without notice to the user, and without probable cause.
- The standard for pen registers is minimal—judges must rubber stamp any application presented to them.
- Many of the protections in the wiretap law, including the special approval requirements and the statutory rule against use of illegally obtained evidence, do not apply to email and other Internet communications.
- ISP customers are not entitled to notice when personal information is subpoenaed in civil lawsuits; notice of government requests can be delayed until it is too late to object.
- Inconsistent standards apply to government access to information about one's activities depending on the type of technology used. For example, watching the same movie via satellite, cable TV, Internet cable modem, and video rental is subject to four different privacy standards.

In addition, there are many ambiguities, some of which have existed since ECPA was enacted, others caused by technology's continuing evolution since 1986. For example, does the pen register statute apply to email or Web communications? If so, what are "the numbers dialed or otherwise transmitted?" To get email addresses and Web addresses (URLs), can the government serve a pen register order on the ISP or must it use an order under ECPA? What information is collected under a pen register order and from whom in the case of a person who is using the Internet for voice communications? What standard applies if the person has a cable modem? Is an Internet portal an electronic communications service under ECPA? Are search terms covered by ECPA? Does ECPA cover government access to information about one's activity at an e-commerce site? Do people have a constitutionally protected privacy interest in their calendars stored on Internet Web sites? At best, the answers are unclear.

The importance of these questions is heightened by the fact that transactional or addressing data for electronic communications like email and Web browsing can be much more revealing than telephone numbers dialed. First, email addresses are more personally revealing than phone numbers because email addresses are unique to individual users. Furthermore, if the pen register authority applies to URLs or

the names of files transmitted under a file transfer protocol, then the addressing information can actually convey the substance or purport of a communication. For example, a search for "heart disease" information through a search engine creates a URL that indicates exactly what content a Web surfer is exploring.

OUTLINING THE NECESSARY PRIVACY ENHANCEMENTS

To update the privacy laws, Congress should start with the following issues:

- Increase the standard for pen registers. Under current law, a court order is required but the judge is a mere rubber stamp—the statute presently says that the judge "shall" approve any application signed by a prosecutor saying that the information sought is relevant to an investigation. Instead, the government should be required to justify its request and the order should issue only if the judge affirmatively finds that the government has shown that the information sought is relevant and material.
- Assuming that the pen register authority applies to Internet service providers, define and limit what personal information is disclosed to the government under a pen register or trap and trace order.
- Add electronic communications to the Title III exclusionary rule in 18 USC § 2515 and add a similar rule to the section 2703 authority. This would prohibit the government from using improperly obtained information about electronic communications.
- Require notice and an opportunity to object when civil subpoenas seek personal information about Internet usage.
- Improve the notice requirement under ECPA to ensure that consumers receive notice whenever the government obtains information about their Internet transactions.
- Require statistical reports for § 2703 disclosures, similar to the reports required under Title III.
- Make it clear that Internet queries are content, which cannot be disclosed without consent or a probable cause order.
- Provide enhanced protection for information on networks: probable cause for seizure without prior notice, opportunity to object for subpoena access.

COMMENTS ON S. 2448

S. 2448 represents an effort to address a range of Internet privacy and security concerns without creating an unwieldy bill. We appreciate the Chairman's decision to stay away from some contentious issues, particularly the Justice Department's request for "roving" pen registers for the Internet, and we hope you will work to keep the bill from being weighted down with other proposals that would expand government surveillance power without adequate privacy standards.

In many ways, we have a robust computer crime law. The Computer Fraud and Abuse Act was originally passed in 1984 and was amended in 1986, 1994 and 1996. It protects a broad range of computers and is quite comprehensive. By its terms, it clearly covers the recent "love bug" virus, the Melissa virus, and the denial of service attacks in February, even those that were created and launched from overseas.

The main effect of S. 2448's criminal provisions would be to extend federal jurisdiction over minor computer abuses not previously thought serious enough to merit federal resources. Currently, federal jurisdiction exists for some computer crimes only if they result in at least $5,000 of aggregate damage or cause especially significant damage, such as any impairment of medical records, or pose a threat to public safety. Any virus affecting more than a few computers easily meets the $5,000 threshold. S. 2448 would eliminate even this low threshold.

Specifically, the bill would make it a felony to send any transmission intending to cause damage or to intentionally access a computer and recklessly cause damage, punishable for up to 3 years in prison, even if the damage caused is negligible. In addition, the bill would make it a misdemeanor to intentionally access any computer and cause damage, even unintentional damage, again regardless of the extent of such damage.

Perhaps unintentionally, these changes would federalize a range of de minimis intrusions on another's computer:

- Somebody borrows a friends computer without permission and changes some files as a joke.
- A student, noticing that someone at the school library's public terminal failed to completely log out of their account, gains access to that student's account and accidentally erases some files.

• A computer science graduate student, in the process of testing a new computer security tool, gains access to another computer on campus without permission and then changes some files to show they were there.

It is highly unlikely that the FBI and the Justice Department could ever have the resources to prosecute such minor computer offenses. The provisions will have to be applied selectively, and the risk becomes high, therefore, that the provisions will be applied in unfair ways.

The elimination of any thresholds is particularly questionable in light of sections of S. 2448 that would amend the forfeiture law in ways that could result in seizure by the government of the house in which sat a computer used in hacking and expand wiretap authority by making all computer crimes a predicate for wiretaps.

Another part of S. 2448 permits the US Attorney General to provide computer crime evidence to foreign law enforcement authorities "without regard to whether the conduct investigated violates any Federal computer crime law." It is unclear whether this expands the Justice Department's investigative authority to investigate lawful conduct in the US at the request of foreign governments.

On the consumer privacy side, S. 2448 has other provisions that would bring about some improvements in privacy, although there are some problems with the bill.

• Sec. 302 would prohibit satellite TV service providers from disclosing information about their customers and their viewing habits unless the customers have affirmatively agreed ("opted-in") to such sharing. This is a step toward addressing one of the many areas of inconsistency in our privacy laws. Currently, federal law protects the subscriber information and viewing habits of a cable TV subscriber but not a satellite TV viewer. Sec. 302 would create privacy protections for viewers of satellite TV. However, we are distressed to see that an exception in Sec. 203 allows disclosure to the government without notice and an opportunity to object, thereby giving satellite TV viewers less protection than existing law affords to cable TVA subscribers.

• Sec. 304 would require commercial Web sites to give visitors notice of data collection and sharing practices and "the opportunity, before the time that such information is initially disclosed, to direct that such information not be disclosed to such person." Again, enforceable requirements of notice and opt-out would be a step forward over current law. However, the bill does not address two other key elements of online privacy—access and security. Further, we believe that it is possible to avoid the current dichotomy between opt-out and opt-in. On the Internet, a better way to think of privacy is in terms of meaningful choice, since the technology can eliminate the transaction costs and other burdens on industry associated with opt-in rules in the offline world. Indeed, some online service providers have adopted in opt-in policy as part of their business mode. given the rapid change that is occurring as businesses respond to persistent high levels of consumer concern about privacy, we would not want federal legislation to freeze opt-out into place.

• Sec. 306 would make fraudulent access to personally identifiable information a crime The provision covers anyone who "knowingly and with an intent to defraud . . . causes to be disclosed to any person, personally identifiable information . . . by making a false . . . statement . . . to a customer of an interactive computer service." The Committee should make it clear whether the "with intent to defraud" language is enough to exclude from the crime a Web site's collection of information under a privacy statement that is not longer being adhered to.

JUSTICE DEPARTMENT PROPOSALS

Our greatest concern, however, is with Justice Department and other proposals for expansions in government surveillance or data access authority. One area of serious concern is Sen. Schumer's bill S. 2092, which, in its current form, extends pen register authority over the Internet in broad and ill-defined ways. S. 2092 also would give every federal pen register and trap and trace order nationwide effect, without limit and without requiring the government to make a showing of need, creating a sort of "roving pen register." We have shared our privacy concerns with Sen. Schumer, along withy our specific recommendations for improvements, and we hope that a more balanced bill could be agreed upon. We have prepared for Sen. Schumer and interested parties a detailed memo, which I would request be made a part of the record of this hearing.

S. 2092 focuses on pen registers, which collect the numbers dialed on outgoing calls, and trap and trace devices, which collect the phone numbers identifying incoming calls. These surveillance devices have long been used by law enforcement in the plain old telephone world. Because they are not supposed to identify the parties to a communication nor whether the communication was even completed, the stand-

ard for approval of a pen register is very low: the law provides that a judge "shall" approve any request by the government that claims the information sought is "relevant" to a investigation. This really says that the court must rubber stamp any government request.

The pen register and trap and trace statute only applies to the numbers dialed or otherwise transmitted on the telephone line to which the device is attached. S. 2092 would extend the pen register and trap and trace authority to all Internet traffic. It does so with very broad terminology, stating that the pen register can collect "dialing, routing, addressing or signaling information," without further definition. It needs to be made clear that pen registers do not sweep in search queries or URLs that identify specific documents viewed online or include personal information.

It is time to give the pen register statute real privacy teeth, requiring the government to actually justify its requests to a judge's satisfaction. Also, if nationwide service is to be available, it should be on the basis of a specific showing of need, and should be limited both by time and other parameters.

CONCLUSION

We do not need a new Fourth Amendment for cyberspace. The one we have is good enough. But we need to recognize that people are conducting more and more of their lives online. They are storing increasing amounts of sensitive data on networks. They are using technology that can paint a full profile of their personal lives. The pricetage for this technology should not include loss of privacy. It should not be the end of the privacy debate to say that technological change takes information outside the protection of the Fourth Amendment as interpreted by the courts 25 years ago. Nor is it adequate to say that individuals are voluntarily surrendering their privacy by using new computer and communications technologies. What we need is to translate the Fourth Amendment's vision of limited government power and strong protections for personal privacy to the global, decentralized, networked environment of the Internet. This should be the Committee's first task.

The CHAIRMAN. Well, thank you, Mr. Dempsey. Let me start with you, but I would like the rest of you to take a crack at this if you care to. In your testimony, you applaud the enhanced privacy provided by the Internet, but doesn't that cut both ways? In other words, does the increased privacy and anonymity afforded by the Internet create greater worries for Americans concerned about Internet crime, such as child pornography or terrorism, or fraud for that matter? Wouldn't you agree that we in Government have some role, perhaps even an obligation, in addressing these concerns?

Mr. DEMPSEY. The Government has a role, obviously. Crime, fraud, child pornography, other criminal activity that is criminal offline is, and should be, criminal online. I think that, again, if you look at the successes of law enforcement, you see that they have been extremely successful in identifying and tracking criminals online, including criminals overseas.

The Citibank computer break-in—the FBI traced the perpetrators of that to Russia and, with the cooperation of Russian authorities, arrested them. Ardita, the Argentine hacker, was traced back to Argentina using online techniques. The Phonemasters, the creator of the Melissa virus—in all of these cases, the Government, using the current authorities that it has and using the current information that is generated, these digital fingerprints that we leave behind, has been successful. Child pornography—obviously, the anonymity there works both ways because you can have an FBI agent go online and pretend to be a 13-year-old girl, and they are making cases in the Innocent Images program.

I think to then try to squeeze that relative anonymity—I don't think there is perfect anonymity on the Internet, never has been and never will be. There are certain forms of relative anonymity

online that are not that dissimilar to some of the forms of relative anonymity that we have offline as we walk down the street.

To try to squeeze out legislatively that remaining bit of anonymity, I think, would have some negative impacts on freedom of expression and privacy. It could have some unintended security implications. Far better to let industry develop the authentication that is required in certain online communications. Other kinds of activity online can proceed anonymously, and I think that is the balance that we need to maintain.

The CHAIRMAN. Thanks.

Mr. Richards.

Mr. RICHARDS. Mr. Chairman, at the Internet Alliance we think consumers and citizens want to know that the cyber cop is on the cyber beat. We think that effective enforcement of current law is absolutely the foundation of what we need today.

The number of law enforcement officials who need to be trained just in the basics of computer forensics are in the single digits, and worldwide it is much worse. So we believe that training, and especially training at the local level, to be frank—the call to 911 should not be met with an unresponsive ear or a blank stare. So this is building for the future for problems we know we will always have, and it begins with the foundations. But we believe that current law is the correct starting place.

The CHAIRMAN. Mr. Heiman.

Mr. HEIMAN. I would echo that. I would say that I think you are hearing agreement here that the sections of your bill which provide funding to beef up the technological capabilities at the FBI, to provide grants to States and locals, to authorize funding for the FBI's NIPC, the National Infrastructure Protection Center, are all a good idea. We really need to do more under the existing laws and authorities and train people how to do that than we do in terms of expanding those authorities right now.

The CHAIRMAN. All right. What would you say is the appropriate role for industry in assuring the security and privacy of Internet users? Should industry take the lead?

Mr. Richards.

Mr. RICHARDS. Mr. Chairman, I think that industry should take the lead, and I think those innovations are already well underway and we are beginning to see them at Internet speed; for example, authentication, easy-to-use means of securing our identity. I might add that, again, going back to current enforcement, we should turn our attention to identity theft, which is not entirely an online issue. In fact, it blends online and offline. These are some of the immediate issues.

But to sum up, we have, I believe, the technologies and the ability to reach users effectively. We are working very hard to do that. If we don't, we ourselves will fail.

Mr. PETHIA. One of the things I think would help industry take its leadership role is additional information from the Government, from the NIPC and others in the FBI, about the kinds of threats that are really there. Industry currently is not moving, I think, quite as quickly as it could, and I think part of the reason is they are not yet convinced that there is a real problem, that there are real criminals, that there is a real smoking gun.

So one of the things that I would encourage in enabling industry to take its leadership role is more information from the Government about the kinds of damages that are being done, the kinds of cases that are being investigated, to the extent that that is possible, and the kinds of threats that are there at the local, the State, and the national level.

Mr. HEIMAN. I would agree with part of that. I certainly think great information from the Government about the threats would really help address this problem. I would say that industry does take the need to improve information security extremely seriously, but it is a tricky problem. I can sort of give you a physical analogy.

We could probably save 20,000 lives a year in the United States by halving our speed limits on the roads, but we don't, and the reason we don't is because the fabric of our lives are such that we need to get from point A to point B in a certain amount of time and we have built up our physical infrastructure in that way.

Well, so too, we depend on the Internet and Internet traffic, and we are not going to stop that traffic. Instead, we are going to do the equivalent of what we do in the physical world. We are going to build safer cars, we are going to improve road conditions, we are going to improve signaling. And so we are going to continue to improve security products, but there is a balance there because you need to maintain the dynamic growth, the vitality, the productivity, and the efficiency of the Internet that is really underlying, for example, much of the economic growth in the 1990's.

The CHAIRMAN. Thank you.

Senator Feinstein.

## STATEMENT OF HON. DIANNE FEINSTEIN, A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thanks, Mr. Chairman. I would like to make a couple of comments, if I might, because I hear a real disconnect in what we are being told by these gentlemen and my experience, and I know some of these individuals and I respect them.

The industry is saying, yes, we need law enforcement; yes, we want privacy; yes, we want all these things, but don't do anything to get us there; we will take care of it. Well, I have been waiting for industry to take care of it for the 8 years since I have been in the Senate and it has not. And, frankly, I was very amazed by the latest report of the FTC because up to 1998, the FTC had been a supporter of that philosophy. And then when they did a survey and they took a look at websites—they looked at 335 commercial web sites, including 91 of the 100 most heavily trafficked websites—what they found is that the number of websites that meet basic standards of privacy protection is far too low.

The FTC said that only 20 percent of the websites of the busiest commercial companies had implemented 4 major information principles: one, notice; two, choice; three, access; and, four, security. Only 20 percent. Moreover, only 8 percent display a privacy seal, a linchpin of any self-regulatory effort. And only 41 percent of the randomly surveyed websites collecting personal information provided consumers information about the site's notice and choice policies.

The Social Security Administration tells us that they have had 30,000 complaints dealing with identity theft involving Social Security numbers, which can be purchased for $49 on commercial Web sites. Personal financial information about an individual that people in this room wouldn't even suspect is available for purchase. Personal health information can also be purchased. And the consumer has no right to know that that is happening.

Mr. Richards, you spoke about your Social Security number being stolen. A staffer came in my office and punched up my Social Security number on a computer; it is up there for sale for anyone that wants to go out and strip my identity. This kind of theft and fraud is on a dramatic increase.

I feel very strongly, Mr. Chairman, that if we are going to move a bill, whatever bill that is, it has to deal with the consumer aspects of privacy. Social Security numbers should not be sold. Now, when you sit down with companies and argue whether it is opt in or opt out, meaning whether a company has the responsibility before they sell a card to notice individuals and ask their permission, the company doesn't want to do this. So they say it is up to the individual to be on guard. Well, I say to them this is my identification number; this is a widely used Federal number. You can't strip me of my number without even telling me you are doing that.

The longer I am around, the longer I watch this dance, and the longer we go around in circles, the more I am concerned by what is happening. Hacking and viruses are one thing, but the public has a basic right to know. The Democratic Caucus a couple of weeks ago had a wonderfully informative lunch—the CEO of eBay came to us, and I marveled at her. She was quite wonderful because she has such high ethical standards. eBay will not allow the information of anyone trading on eBay to be sold or used in any other way. But that is a rare instance.

Most of the time, all of this material is up for sale. So the sophisticated person can actually use it, buy it, develop full profiles about people that they want to go out and defraud, steal their identity, use their credit cards, pretend they are them. And you even have complaints to the Social Security Administration going from 11,000 complaints in 1998 to 30,000 complaints in 1999. That number is going to double again and again and again.

So what I heard all you gentlemen saying is the laws are adequate. But this isn't petty larceny with a prior, this isn't grand theft, this isn't robbery, this isn't burglary. Our laws aren't adequate to deal with this.

Mr. DEMPSEY. Senator, could I respond?

Senator FEINSTEIN. Absolutely.

Mr. DEMPSEY. At the Center for Democracy and Technology, we have come to the point that you have come to, and we do believe that Federal legislation is necessary to address the privacy concerns of consumers, for all of the reasons that you state, including that recent FTC report, and for a further reason, which is there are now 700 bills pending at the State legislatures to address consumer privacy online and offline.

That says to us that it would be chaos to have 50 different State rules for privacy online, on a borderless medium. So we are going to have to get to the point, and the chairman's bill has a provision

in it addressing two of the four items that the FTC report calls fundamental principles of privacy. The chairman's bill addresses notice and choice. It does not address the other two that you mentioned, access and security, which are very hard issues. All these issues actually are hard, but the last two are the hardest.

If I could just for one second, on the question of choice—and you mentioned the opt-out versus opt-in debate. This is the classic case where this technology and its interactive nature can eliminate much of that debate, can eliminate much of that concern. It is so easy to present online meaningful choice to consumers. Whether you call it opt-in or opt-out, right there the consumer can be told this is our policy, this is what we want from you, these are your choices, do you agree, don't you agree.

Senator FEINSTEIN. Let me interrupt you. My Social Security number is my number. How can somebody sell that number to those who may abuse it, or sell it? Why does anyone want to protect that?

Mr. DEMPSEY. I don't think it should be protected, Senator. We used to have a law in this country that said that the Social Security number is to be used only for the purposes of administering the Social Security system. You give it to your employer for purposes of taxes and it goes to the Social Security Administration so they can match up who you are and what your benefits are. That was the purpose of that number when that system was first created.

Senator FEINSTEIN. That is correct.

Mr. DEMPSEY. Over time, we created exception after exception after exception. Thirty States now use that number on their driver's license. Multiple instances——

Senator FEINSTEIN. But nobody sells it. Until recently, no one has sold it.

Mr. DEMPSEY. Well, actually, Senator, Congress actually had to pass a bill. The States were selling that information. The States were selling the driver's license information. In 1994, this committee passed the Driver's Privacy Protection Act to begin to try to clamp down on that.

Last year, this Congress strengthened that Act because then the States started selling the pictures off of the—or planning to sell the digital pictures off the driver's license. That has now been shut down, but it took an effort to basically put that cat back in the bag. But now your Social Security number, because we have gotten blase about it, is out there on multiple different forms. Possibly, some filing you made as a Senator included your Social Security number and someone took that off of there.

Senator FEINSTEIN. Well, let me ask you a question. Would your Center support legislation that would make it illegal to sell a Social Security number without the individual's permission?

Mr. DEMPSEY. I think that is something that we have to move toward, and I am not going to right now say what it is.

Senator FEINSTEIN. There you go.

Mr. DEMPSEY. No. What I am saying is to make it illegal to sell the number——

Senator FEINSTEIN. Wherever you sell it, period, making it illegal to sell somebody's number offline or online.

Mr. DEMPSEY. I think I want to work with you on that and I want to come up with a bill with you.

Senator FEINSTEIN. It is pretty simple.

Mr. DEMPSEY. With all respect, Senator, drafting a criminal law on the sale of information is not that easy. If it is already out there in the public domain, I think we need to think it through.

Senator FEINSTEIN. OK, all right.

Mr. DEMPSEY. I am a hundred percent with you that this is an issue. We have lost control over the Social Security number. It is terrible the way these numbers are now being sold and then used as the basis for identity theft. We need to get control over that. What actually that mechanism is I am not prepared to write that bill right this second. I will write it this afternoon if you want, but not right here.

Senator FEINSTEIN. Well, I appreciate that because I will be introducing such a bill. Senator Grassley and I are working together on the issue. Senator Kyl and I are also working on a bill on cyber crime, Mr. Chairman. If S. 2448 is the bill you intend to move, I hope you would take a look at some of the concepts I have mentioned.

I think if we are going to pass a privacy bill, the consumer has to be protected. A privacy bill has to be good for people. We have got to achieve some protection for people's privacy, their financial data, their health data, Social Security numbers, whether drivers' license pictures or information should be sold.

I think too much identity theft is happening, and there is now evidence that some of these thefts are actually being used to carry out crimes of murder. Now, murder can be currently prosecuted. The law provides for that, but everything involved in indentity theft can't be prosecuted as clearly as murder.

I don't want to belabor the point, Mr. Chairman, but if you would be so good, as you always are, to take a look at our bills and see if they might meet muster, I would appreciate it.

The CHAIRMAN. I will be glad to do it.

Senator FEINSTEIN. I also have a statement I would like to put in the record, Mr. Chairman.

The CHAIRMAN. It will be included in the record.

[The prepared statement of Senator Feinstein follows:]

PREPARED STATEMENT OF SENATOR DIANNE FEINSTEIN

I am grateful to the Chairman for this hearing because he correctly links the security of our nation's electronic infrastructure with personal privacy. In both cases, we are trying to stop unlawful and inappropriate disruption and invasion. Just as our nation's websites are subject to attacks from viruses like the "I love you" virus, our privacy can also be subject to attack on the Internet.

Few would contest that the protection of personal privacy is a key concern of many Americans as they consider the growth of the Internet.

That is because, for the first time, the Internet permits a company to browse a shopper, while a shopper is browsing in the store. Information brokers can compile dossiers on people. These dossiers are growing ever larger and more precise. To safeguard the future of the Internet, we must safeguard the privacy concerns of people who use it.

I am encouraged by the Federal Trade Commission's announcement this week that privacy legislation is needed. The devil, of course, is in the details.

When considering Internet privacy or privacy in the "off-line" world, I think, as a basic principle, people should have more control over the information they consider personally sensitive.

As on small step in this direction, I am pleased to announce that I am working with Vice President Al Gore, who has a keen personal interest in this matter, on an Administration bill that would prohibit the sale of Social Security numbers, whether they are sold on the Internet or off the Internet.

*History of interest in privacy of SSNs*

My reservations about the trafficking in SSNs have deep roots. In 1997, I introduced S. 600, the Personal Privacy Information Act, after watching in dismay as one of my staff downloaded my SSN off the Internet in less than a minute.

Not much has changed. For a mere $49, one can go on-line and purchase a person's SSN from a whole host of web businesses—no questions asked.

*Threat posed by sale of SSNs*

Why is it so important to stop this sale of SSNs? Once a criminal has a potential victim's SSN, that person is extremely vulnerable, subject to having her whereabouts tracked and her identity stolen. Though never intended to be anything more than a tool for the Social Security Administration to track personal earnings, the Social Security number has become a de facto national identifier. It is the key to one's public identity.

The Federal government uses the SSN as the taxpayer identification number, the Medicare number, and as a soldier's serial number. Many states use the SSN as the identification number on drivers' licenses, fishing licenses, and other official records. Banks use it to establish personal identification for credit. The number is requested by telephone companies, gas companies, and stock brokerages when consumers set-up personal accounts. Supermarkets ask for the number when an applicant wishes to get a check-cashing card.

If you believe that these number are kept confidential by government and commercial providers, think again. Without any restrictions, third parties can buy SSNs off the Internet. In those states where SSNs are on driver's license, if your wallet is stolen, so is your SSN. Credit bureaus sell SSNs by the thousands. One's SSN is anything but private or confidential.

Thus, SSNs have the dubious distinction of being easy for criminals to obtain and, at the same time, the most common tool used for identifying people.

*Identity theft*

Partly due to this unrestricted traffic in SSNs, our country is facing an explosion in identity theft crimes. The Social Security Administration recently reported that it had received more than 30,000 complaints about the misuse of Social Security numbers last year, most of which had to do with identity theft.

This figure is up from 11,000 complaints in 1998 and just 7,868 in 1997. In total, Treasury Department officials estimate that identity theft causes between $2 and $3 billion in losses each year—just from credit cards alone.

Sometimes, this unrestricted sale of personal information can have tragic results. Amy Boyer, a twenty-year old dental assistant in New Hampshire, was killed by a man who tracked her down through the online personal-data service Docusearch.com

*Administration bill's impact*

The legislation I am working on with the Administration will stop the unrestricted sale of Social Security numbers. It will prevent people like Amy Boyer's killer from logging onto an Internet site and purchasing her Social Security number. It will make it harder for criminals to use your SSN as a stepping stone to assuming your identity.

*Future legislation*

In addition to this joint effort with the Clinton Administration, I also am working with Senator Grassley on a broader initiative to cut down on the misuse of SSNs.

This expanded proposal will prevent companies from denying service to those individuals who refuse to give a company their SSNs. The bill will prohibit government agencies from disclosing SSNs on mailing labels or other public documents. The legislation also will enhance the Social Security Administration's ability to prosecute criminals who misuse SSNs by adding civil penalties to existing criminal penalties.

The CHAIRMAN. I appreciated your testimony. I am going to submit questions to you.

[The questions of Senator Hatch can be found in the appendix.]

The CHAIRMAN. I am not advocating that Government is or should be the solution to the Internet security and privacy concerns

concerning the Internet. I think the Government should do what it can within what I consider its traditional limited role to help industry protect the infrastructure and to help deter malicious attacks on the Internet and a network that we rely on.

I am skeptical of, and in fact oppose at this point, efforts to regulate privacy on the Internet. I have devoted my whole career to end unneeded regulations that we have on the books that raise the cost of doing business and that distort the marketplace and end up limiting choices for consumers.

I agree with Senator Feinstein that an effective security and privacy regime should protect consumers, to the extent the consumer expects it. And in doing so, it strives to restore the consumer's confidence in the integrity of the Internet. I think it should also be flexible enough to allow for variances in consumer expectations and marketplace solutions as well.

To date, the discussions surrounding Internet privacy have revolved around two mutually exclusive models as possible solutions to this issue. The first, advocated by certain consumer rights groups and now by the FTC, would give government regulatory bodies the authority to regulate conduct on the Internet. And the second, advocated by most members of the industry, would entrust the industry to regulate itself without any role for the government.

As I suggested last year, one solution worth considering is the possibility of establishing a private sector board with limited government oversight to address the security and privacy concerns, while taking into consideration the special characteristics of the Internet. The board might set some basic rules and let the marketplace determine how those rules will be complied with. That is at least a thought that I have.

Frankly, this is a very intriguing area to me, as I am sure it is to all of you. And I would like to have your best suggestions and advice as to what this final legislation should be. We have filed it. We want your comments. We want to change things that aren't quite accurate or right. Of course, that is the reason for hearings and that is the reason for this whole legislative process. But I intend to have a privacy bill through by the end of this year, and we would like your help in doing so and we would like to do it in a way that would really help everybody concerned.

With that, we will keep the record open until 6:00 today for anybody to submit any questions that they would like, and I would hope that you would get your answers back as quickly as you can because this is important and I am going to move forward with this bill. I will, in the process, also take Senator Feinstein's advice to look at these other legislative measures and see if we can dovetail those with this bill as well.

Thank you. Your testimony has been very important to us, and we appreciate your making the effort and taking the time to do this. Thanks so much.

We will include in the record all statements submitted by the members of the committee.

[The prepared statement of Senator Thurmond follows:]

PREPARED STATEMENT OF HON. STROM THURMOND, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Mr. Chairman: I am pleased that we are holding this hearing today regarding the threat of serious criminal misconduct involving the Internet.

A few months ago, hackers essentially shut down some popular and important Internet sites temporarily by overwhelming them with data. My Subcommittee on Criminal Justice Oversight, in conjunction with the House Judiciary Crime Subcommittee, held a hearing on these denial of service attacks and discussed the need to tighten our laws regarding computer crime. Very recently, serious damage was caused to computers around the world by the "I Love You" virus, which apparently was unleashed in the Philippines. The technology used in these attacks was not very complex, which raises the question of what hostile adversaries could accomplish through a sophisticated, concerted effort.

Internet crime is a serious, growing threat. Law enforcement must have the tools and resources it needs to address this problem. Also, our criminal laws must be updated as needed so that they remain technology neutral. Punishment must be as swift and severe in the computer world as it is in the real world. There can be no double standard regarding crime on the Internet.

The private sector, which controls 90 percent of the infrastructure, should take the lead in protecting computer systems from attacks, just as citizens must protect themselves from crimes by locking their doors. Also, industry should cooperate with law enforcement and share information regarding intrusions with the authorities and among themselves. It is critical for industry to view the government as a partner in their joint efforts to stop malicious hackers and other Internet crime.

I welcome our witnesses to discuss this important, timely issue.

[The prepared statement of Senator Grassley follows:]

PREPARED STATEMENT OF HON. CHARLES E. GRASSLEY, A U.S. SENATOR FROM THE STATE OF IOWA

Mr. Chairman, I'd like to raise a serious concern I have about NIPC. The General Accounting Office recently did a review of NIPC's performance. It looked in particular at the ILOVEYOU virus, and NIPC's response to that.

The White House issued a "white paper" on the Presidential Decision Directive that governs the NIPC. According to that paper, the mission of the NIPC includes "timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response."

The GAO review was critical of the NIPC. It noted that NIPC did not issue an alert on its Web site until 11 am on May 4. This was hours after the rest of the world already knew. My own office was notified before 9 am, two hours before NIPC issued its alert. And, it wasn't until 10 o'clock at night that advice on how to deal with the virus was posted by NIPC.

Here's what the GAO said about NIPC's performance:

"The lack of more effective early warning clearly affected most federal agencies. . . . Clearly, more needs to be done to enhance the government's ability to collect, analyze and distribute timely information that can be used by agencies to protect their critical information systems from possible attack. In the ILOVEYOU incident, NIPC and FedCIRC, despite their efforts, had only a limited impact on agencies being able to mitigate the attack."

Now, this program to protect the nation's critical infrastructure has a $40 million budget. And the bill before this committee would increase and extend that budget for another five years. That's section 402. And I'm a little concerned about that.

The program was supposed to be a clearing house for information from all sources, and a focal point to coordinate the investigations of various federal law enforcement agencies. The private sector participation is intended to be voluntary.

But the private sector has not participated. That's because they can't get information or cooperation from the FBI. And many of the agencies have pulled out. Most notably Treasury and Commerce. That's because all the incoming cases have been taken by the FBI. The PDD calls upon them to distribute cases according to expertise. That's not being done.

Getting information out of the NIPC is also pretty tough. GAO briefed me last week that NIPC hadn't responded formally to its request for information about the ILOVEYOU incident. That was after nearly three weeks of asking. Other agencies responded within 24 hours.

Two months ago at a hearing before this committee, I submitted follow-up questions for NIPC. I have yet to hear back.

And now, some Senators on this committee, myself included, have asked for an audit by GAO, and an investigation into whether NIPC is fulfilling its charter. This will be a major undertaking by GAO. And I think members of the committee will want to see the results. So I would urge caution about funding the program without making some much-needed changes.

Most important, I think, in fueling the problems we've encountered with this program is how the FBI handles a case. The FBI doesn't share information when it's working on a case. And rightfully so. But the point of responding to critical incidents like the ILOVEYOU case is to share information rapidly. The two methodologies are incompatible. That's why the PDD intended the program to operate as a cooperative effort. But that's not the way it's being carried out.

So, I just wanted to take this time, Mr. Chairman, and raise these concerns. I have no questions of Mr. Vatis at this time. But I do look forward to getting answers to my questions from March. And I hope that happens very soon.

[The prepared statement of Senator Kyl follows:]

PREPARED STATEMENT OF HON. JON KYL, A U.S. SENATOR FROM THE STATE OF ARIZONA

As we all know, the Information Age continues to change the way we live. Millions of American's log on to the Internet every day to shop, to communicate with friends, to buy and sell stocks, and so on. Computer networks and the Internet also form the backbone of critical services Americans depend on every day, like the electricity grid, telecommunications, air-traffic control, and military early warning systems.

Several events in recent weeks have highlighted the fact that the benefits of the Information Age have been accompanied by new challenges. The denial of service attacks earlier this year on popular e-commerce web sites and the recent spread of the "I Love You" virus have awakened most Americans to the need for improved cyber security—something that many experts have been warning about for some time.

Over the past three years, I've chaired seven hearings on cyber security issues in my Subcommittee. It's clear to me that there are responsible things we can and should do in the Congress to improve cyber security. In many cases, this merely entails updating our laws to reflect the current state of technology development.

For example, Senator Schumer and I have introduced a bill to improve the ability of law enforcement agencies to investigate cyber crimes. The key provision of this bill would remove the requirement for law enforcement to obtain a court order in every jurisdiction in order to trace hacking attacks that, in many cases, are purposefully routed through several Internet service providers in different states to make it difficult to trace. In dealing with the Internet, which knows no boundaries, the requirement for a separate court order in every jurisdiction simply no longer makes sense. One court order authorizing nationwide trap and trace authority will improve investigation of computer crimes while maintaining the ability of our judicial system to protect the civil liberties of Americans.

Mr. Chairman, I look forward to continuing to work with you and the other Members of the Committee to address these important issues and I thank you for the opportunity to make this brief opening statement.

The Chairman. With that, we will recess until further notice.

[Whereupon, at 12:22 p.m., the committee was adjourned.]

# APPENDIX

## QUESTIONS AND ANSWERS

### RESPONSES OF BRUCE HERMAN TO QUESTIONS FROM SENATOR HATCH

*Industry role*

*Question 1.* What is the appropriate role of industry in assuring the security and privacy of Internet users? Should they take the lead?

Answer 1. Yes, industry should continue to lead the effort to make the Internet more secure Industry-led, market-driven solutions to Critical Information Infrastructure Protection have the best prospects of success. Moreover, a voluntary cooperative partnership between industry and government is the only approach that can work.

Specifically, the private sector can do three things. First, industry can constantly improve protection of its product lines and networks. Private companies are in the best position to know how to protect infrastructures they have developed, owned and operated. But it is important to understand that there is no one single "silver bullet" for the problem of information security—rather, it is a process of continual improvement.

Second, the private sector must continue to educate the public on the need to practice good "security hygiene" and to educate others to do so. The private sector needs to continue to spread the message that, just as you wouldn't let anybody into your house, so you shouldn't let just anybody into your computer.

Third, industry does need to share information among itself and with the government about threats and vulnerabilities as well as best practices. In this regard, ACP has met with representatives of the National Security Council staff, the FBI's National Infrastructure Protection Office (NIPC), and the Dept. of Commerce's Critical Infrastructure Assurance Office (CIAO), and ACP has been encouraged to continue the dialogue.

*Question 2.* To what extent is it necessary for industry to involve law enforcement in taking steps to ensure the security and integrity of the Internet? Could the use of encryption devices, for example, in fact frustrate the ability of law enforcement to provide assistance when such assistance is requested by industry or required under law?

Answer 2. Industry should involve law enforcement to help prevent, investigate, and prosecute computer crime that threatens the security of the Internet. Toward this end, industry should share information with law enforcement about threats and vulnerabilities. ACP also supports giving law enforcement the requisite resources and training to investigate and prosecute cyber crime.

But, of course, it is up to the private sector in the first instance to protect itself by adopting good security measures. Encryption is an essential component of information security. That is why ACP was pleased by the widespread Congressional support for liberalizing export controls on American encryption products that helped lead to the Administration's new regulations in January. The widespread use of encryption helps prevent crime, as well as protect national security and promote the privacy of Americans at work and at home.

*Government regulation*

*Question 1.* A primary criticism of government regulation of privacy on the Internet is that it would stymie technologic innovation of this industry. Do you agree with this criticism? If you do agree, please describe how this might occur.

Answer 1. Yes. ACP strongly opposes government efforts to mandate the use of particular technologies or to insist on certain design standards in order to allegedly protect our nation's critical information infrastructure. It is the private sector that owns and operates the networks, systems, products and services that constitute the information infrastructure and it is the private sector that has the experience and expertise to protect it. New laws or regulations would stifle innovation, artificially channel R&D, and harm the very infrastructure that needs protection.

ACP also strongly believes government must not violate personal and corporate privacy in the quest for Critical Information Infrastructure Protection. Indeed, as more of our lives are conducted electronically, it is essential that we ensure the security and privacy of information, communications and transactions from unjustified and unwarranted government examination. The government must not increase widespread surveillance or monitoring of Americans at home and work.

*Question 2.* In addition, it is your opinion that any government action would hurt technologic innovation? What actions can the government take to both encourage technoligic innovation and address the issue of consumer privacy on the Internet?

Answer 2. See answers to other questions.

*Use of consumer information*

*Question 1.* Given what an important resource the Internet is for companies to target potential consumer groups, are there ways a consumer's personal information could be made available to third parties for business purposes while still maintaining a consumer's anonymity and privacy?

Can the government take any actions that might help industry do this? If so, what?

Answer 1. ACP focuses on the interaction of the private sector with the government. ACP led the private sector to liberalize export controls on American encryption products and is now focused on the right way to protect America's critical information infrastructure. ACP has not addressed the topic raised by this question.

*Privacy concerns*

*Question 1.* National polls indicate that personal privacy is an increasing concern amongst consumers as the Internet is being used more and more each day to conduct personal business such as purchasing consumer goods, banking, and trading.

In your view, are such privacy concerns justified?

Will commerce on the Internet reach its full potential if such concerns are not adequately addressed?

Answer 1. ACP has focused on privacy rights of Americans vis a vis their government. We are concerned about the potential for governmental abuse of the increasing amount of electronic personal information. Thus ACP supports giving law enforcement the requisite resources and training to investigate and prosecute cyber crime. But we oppose the initiation or increase of widespread government monitoring or surveillance of Americans by the government. Just because we know that some will commit cyber crime, it would be wrong to watch closely what everyone is doing.

ACP as an organization does not have a position on commercial privacy issues. They are not within the organization's mission (see attached mission statement). However, we recognize that these issues are complex and controversial—and are concerned about a single bill that addresses both commercial privacy and cyber security/infrastructure protection (as does S. 2448). Moreover, we know that many members of ACP individually and through other organizations have implemented privacy policies and are adopting privacy enhancing technologies and have concerns about the commercial privacy provisions of S. 2448.

*Privacy protections—individuals vs. business*

*Question 1.* In the analog world there are different expectations of privacy in different concerns. For example, there is a substantial difference in privacy expectations between the shopkeeper and the shopper. Certainly a consumer would expect to be able to shop for a computer without surrendering significant personal information. But one does expect to have access to sufficient information about the seller to verify that it is a reputable dealer. Such information may be even more important in the virtual world where certain unscrupulous shopkeepers can hide behind technologically-rich facades that give then an aura of credibility.

Does this not suggest we protect privacy of online shoppers and web surfers, and require disclosure from web site proprietors, especially those engaged in e-commerce, or at least that we should treat differently the privacy claims of people surfing the net and those holding themselves out on the net by opening web sites?

Answer 1. ACP as an organization does not have a position on commercial privacy issues. They are not within the organization's mission (see attached mission statement).

---

RESPONSES OF BRUCE HEIMAN TO QUESTIONS FROM SENATOR LEAHY

*Question 1.* Do you support or endorse S. 2448? Are you aware of any companies or organizations that support or endorse S. 2448?

Answer 1. ACP does not support S. 2448 as introduced. We are not aware of any companies organizations that endorse the bill.

*Question 2.* Please comment on your views of S. 2448 and explain any specific concerns you may have about this legislation.

Answer 2. As a first principle, ACP does not believe Congress should rush to pass legislation in the area of critical infrastructure protection. Indeed, we believe premature legislation could prove counter-productive. We outlined our specific concerns about S. 2448 in a letter to Chairman Hatch (see attached). Essentially, ACP supports giving law enforcement the requisite resources and training to investigate and prosecute cyber crime. We believe this can be accomplished through the appropriations process. We do not believe there is a need for new authorizing legislation, particularly a bill that would give broad new authorities to the government or expand existing authority (such as trap and trace) to new areas (such as the Internet) without much more detailed examination of all the potential ramifications.

*Question 3.* In my opening statement, I gave the example of the college student who without authorization accesses his professor's computer to see what grade he is going to get and accidentally deletes a file or a message. That conduct may be cause for discipline at the college but would not be a federal crime under current law, unless the conduct caused over $5,000 in damage. (A) Do you think that sort of unethical conduct warrants federal law enforcement attention and should be a federal crime?

Answer 3A. Cyber crime is a serious problem—whether hacking, unleashing a virus, or pirating copyrighted material. I cannot be treated casually. At the same time, prosecutors are already stretched thin. The question is one of balance. Without commenting on the $5,000 threshold, this particular conduct does not seem worthy of federal law enforcement attention. It involves neither conduct that is interstate in nature nor any other serious federal interest.

*Question 3B.* Under S. 2448, this unauthorized access to the professor's computer would constitute a felony violation of 1030(a)(5)(B), punishable by up to 3 years' imprisonment, with a mandatory minimum of at least 6 months in jail, or a misdemeanor violation of 1030(a)(5)(C). Rather than trust federal prosecutors to exercise their discretion to decline such a case, would it be preferable for Congress to define clearly what should and should not be a federal crime?

Answer 3B. ACP does not have a position on this issue.

*Question 4.* Some have suggested that some change to the Freedom of Information Act (FOIA) would be useful to encourage private sector cooperation with the government in protecting critical infrastructures. I have long supported the FOIA as a critical tool for all Americans to find out what their government is doing. This is healthy and necessary for our democracy. Consequently. I am concerned about proposals that allow agencies to keep "secret" broad categories of records in their possession that may be related to the "critical infrastructure" and to block FOIA requests, with no other justification and no judicial review. This would certainly reduce the FOIA workload of Federal agencies, but labeling information as related to "critical infrastructure" as a means of exempting entire categories of information from the FOIA would, in my view, undercut and pose a threat to the effectiveness of the FOIA.

Answer 4. There is an on-going, serious discussion within industry itself and between industry and government about the possible need for legislation to facilitate the sharing of information among the private sector and between the private sector and government. Such legislation could provide enhanced protection of shared information by removing disincentives for this dialogue. An FOIA exemption is only one such measure. The possible application of the antitrust laws is another. Finally, there is the disincentive resulting from the apparent ability of third-parties to use disclosed information against those who provide it. ACP is carefully reviewing legislation introduced in the House by Reps. Davis and Moran.

*Question 4A.* Would you agree with me that any change to the FOIA must avoid undercutting the usefulness of the FOIA and ensure the effectiveness of judicial review?

Answer 4A. No response.

*Question 4B.* What suggestions, if any, do you have for refining the FOIA in ways that would narrowly address the legitimate concerns of the private sector about sharing information to protect our critical infrastructures while at the same time maintaining the presumption in FOIA that federal agency records are subject to the disclosure and that agency action is subject to judicial review?

Answer 4B. No response.

---

RESPONSES OF RICHARD PETHIA TO QUESTIONS FROM SENATOR HATCH

*Question 1.* What is the appropriate role of industry in assuring the security and privacy of Internet users? Should they take the lead?

Answer 1. Technology vendors and Internet service providers of all forms have a responsibility to insure that the products and services they produce and offer in the Internet community are fit for use in that environment. That means they have a responsibility to fully understand the risk and threats in that environment and to take steps to insure their products and services effectively mitigate those risks when used appropriately by their customers. To date, it is not clear to me that the industry is taking its responsibility seriously. Security incidents are increasing, the damage from those incidents is increasing, and the vunlerabilities discovered in internet technology products are also on the increase. In this area, I believe the appropriate step for government to take is to insure it takes no steps to limit the liability of Internet product and service providers with respect to damages caused by their offering of products and services that are not fit for use in the Internet environment. Allowing the marketplace and the civil courts to freely handle the issues of fitness for use, damage and liability is the best way to send a strong message to industry that they will be held accountable for the consequences of reasonable use of their products.

*Question 2.* To what extent is it necessary for industry to involve law enforcement in taking steps to ensure the security and integrity of the Internet? Could the use of encryption devices, for example, in fact frustrate the ability of law enforcement to provide assistance when such assistance is requested by industry or required by law?

Answer 2. As the Internet grows and becomes increasingly accessible to the entire global community, we are sure to see many of the criminal problems we see in other aspects of our lives. In fact, because the Internet is such a powerful tool, we are likely to see new forms of crime where criminals take advantage of the power of the net to achieve their purposes. Just as industry does not have the ability to deal with all forms of crime today, it will not have the ability to do so on the Internet. Law enforcement will play a necessary and important role. At the same time, it is important to understand that the Internet is changing the rules of the game in many aspects of our societies. It will change the rules in law enforcement as well. Using your example of encryption, it has historically been the case that only governments have had access of strong encryption. The Internet, along with the global spread of technical capability, has changed this. Today, strong encryption products are available from a variety of global sources. The Internet assures that these products are accessible globally and inexpensively. In this case, and I'm sure we will see others as well, the technology genie is out of the bottle and will not go back in. Law enforcement, along with the rests of us, will need to recognize that the Internet (as an example of all new forms of information technology) will obsolete old ways of doing business (whatever that business is) and push us to find new ways to meet our responsibilities.

*Question 3.* A primary criticism of government regulation of privacy on the Internet is that it would stymie technologic innovation of this industry. Do you agree with this criticism? If you do agree, please describe how this might occur. In addition, is it your opinion that any government action would hurt technologic innovation? What actions can the government take to both encourage technologic innovation and address the issue of consumer privacy on the Internet.

Answer 3. I agree that there is some risk the government regulation of privacy on the Internet could stymie innovation, but believe that risk is limited if the government regulations focus on outcomes rather than specific technical mechanisms. For example, many organizations, both inside and outside the Internet community, collect information about their customers and about their customer's use of their products. The issue of privacy focuses on how they protect, use, and further disseminate that information. Government regulations could require organizations to control access to the information, disclose how it is to be used, and further disseminate it only in an aggregated form where it is no longer possible attribute data elements

to individuals. This type of regulation is silent on the technology, but still brings protection for individual's privacy. It is then up to industry to become even more innovative and develop cost effective ways to support the regulations. In general, I believe regulations focused on technology will stymie innovation. Regulations focused on outcomes should not have that effect.

*Question 4.* Given what an important resource the Internet is for companies to target potential consumer groups, are there ways a consumer's personal information could be made available to third parties for business purposes while still maintaining a consumer's anonymity and privacy? Can government take any actions that might help industry do this? If so, what?

Answer 4. I have no good ideas on this one. It seems to me that information about individuals can either be distributed (and their privacy affected) or not.

*Question 5.* National polls indicate that privacy is an increasing concern among consumers as the Internet is being used more and more each day to conduct personal business such as purchasing consumer goods, banking, and trading. In your view are such privacy concerns justified? Will commerce on the Internet reach its full potential if such concerns are not adequately addressed?

Answer 5. In my view, the concerns are justified, but the focus on the Internet is off-base. I believe that what we are seeing in an entire new industry focus on collecting and disseminating information about individuals. For example, my supermarket offers a card that I can use for discounts when I use it at the check-out line. What this card does is remove my anonymity with respect to the purchases I make. It allows my supermarket (and anyone they give/sell the information to) to develop a profile of my purchasing patterns and my individual product preferences. On the positive side, they can use this information to better inform me of products that have the characteristics I prefer. On the negative side, they can use this information to describe products to me in a way that makes it appear they have the characteristics I prefer even if they do not really have these characteristics. At the base, this is not an Internet issue. It is an issue of collecting and disseminating information about individuals. If there are to be any regulations, they should focus on this, and issues such as truth in advertising, rather than the more narrow focus on the Internet. In these cases, the Internet simply facilitates good and bad practice. There is nothing inherent in the Internet that favors either one.

*Question 6.* In the analog world there are different expectations of privacy in different contexts. For example, there is a substantial difference in privacy expectations between the shopkeeper and the shopper. Certainly a consumer would expect to be able to shop for a computer without surrendering personal information. But one does expect to have access to sufficient information about the seller to verify that it is a reputable dealer. Such information may be even more important in the virtual world where certain unscrupulous shopkeepers can hide behind technologically-rich facades that give them an aura of credibility. Does this not suggest we protect the privacy of on-line shoppers and web surfers, and require disclosure from web site proprietors, especially those engaged in e-commerce; or at least that we should treat differently the privacy claims of people surfing the net and those holding themselves out on the net by opening web sites.

Answer 6. The problems we face in the virtual world are basically the same as those we face in the analog world with the exception that state and national boundaries no longer have meaning. In the analog world, we all face the problem of unscrupulous merchants (e.g. home improvement charlatans, financial scams of one form or another, rip-off at the auto shop, etc). We face the same problems in cyberspace compounded by the lack on national boundaries and the fact (as you suggest) that it takes very little capital to establish what looks like a credible store-front. In these cases, "buyer beware" becomes even more important. Here I think the best thing the government can do is develop awareness campaigns that inform consumers of the risks in the virtual world. It can also foster the development of things such as "better business bureaus of cyberspace" and "cyberspace consumer reports" to help consumers separate the credible from the corrupt. This ongoing "registry" of information on the quality of Internet product and service providers will be a massive on-going effort that requires industry participation and support. I think this, rather than requiring disclosure (which itself could be false and how are you ever going to police it all internationally) from web site operators, is more likely to give consumers the information they need and build consumer confidence.

RESPONSES OF JEFF B. RICHARDS TO QUESTIONS FROM SENATOR LEAHY

*Question 1.* Do you support or endorse S. 2448? Are you aware of any companies or organizations that support or endorse S. 2448?

Answer 1. As we have stated in prior comments to the Committee, we do not support or endorse passage of this legislation at this time. In particular, with respect to privacy legislation, we believe that the combination of voluntary, industry-led privacy programs coupled with emerging technology, will deliver more flexible, more meaningful, and ultimately more satisfying privacy protection to the public than the application of one-size-fits-all legislative approaches. We cannot speak for other associations or companies.

*Question 2.* Please comment on your views of S. 2448 and explain any specific concerns you may have about this legislation.

Answer 2. These views and concerns were expressed in our testimony before the Committee on S. 2448, and in our letter to the Committee of June 23, 2000. We refer you to these documents.

*Question 3.* In my opening statement, I gave the example of the college student who without authorization accesses his professor's computer to see what grade he is going to get and accidentally deletes a file or message. That conduct may be cause for discipline at the college but would not be a federal crime under current law, unless the conduct caused over $5000 in damage. a. Do you think that sort of unethical conduct warrants federal law enforcement attention and should be a federal crime?

Answer 3a. As stated in our letter and testimony, we feel the current $5000 damage requirement, if augmented by the law enforcement's ability to aggregate damages to multiple computers or networks, would serve the public interest better than elimination of the $5000 requirement.

*Question 3b.* Under S. 2448, this unauthorized access to the professor's computer would constitute a felony violation of 1030(a)(5)(B), punishable by up to 3 years' imprisonment, with a mandatory minimum of at least 6 months in jail, or a misdemeanor violation of 1030 (a)(5)(C). Rather than trust federal prosecutors to exercise their discretion to decline such a case, would it be preferable for Congress to define clearly what should and should not be a federal crime?

Answer 3b. Yes, generally we feel it preferable for Congress to define clearly what should and should not be a federal crime. For further insight on our section 1030 comments, see our letter of June 23.

*Question 4.* Some have suggested that some change to the Freedom of Information Act (FOIA) would be useful to encourage private sector cooperation with the government in protecting critical infrastructures. I have long supported the FOIA as a critical tool for all Americans to find out what their government is doing. This is healthy and necessary for our democracy. Consequently, I am concerned about proposals that allow agencies to keep "secret" broad categories of records in their possession that may be related to the "critical infrastructure" and to block FOIA requests, with no other justification and no judicial review. This would certainly reduce the FOIA workload of Federal agencies, but labeling information as related to "critical infrastructure" as a means of exempting entire categories of information from the FOIA would, in my view, undercut and pose a threat to the effectiveness of the FOIA. a. Would you agree with me that any change to the FOIA must avoid undercutting the usefulness of the FOIA and ensure the effectiveness of judicial review?

Answer 4a. To date we have not taken a position on any specific proposal to amend FOIA. We are aware that the Partnership on Critical Infrastructure and the Digital Private Sector Working Group, among others, are studying this question and will be reporting recommendations. We urge Congress to defer any legislation along these lines until the reports of these groups are available.

*Question 4b.*What suggestions, if any, do you have for refining the FOIA in ways that would narrowly address the legitimate concerns of the private sector about sharing information to protect our critical infrastructures while at the same time maintaining the presumption in FOIA that federal agency records are subject to the disclosure and that agency action is subject to judicial review?

Answer 4b. As noted in the answer to the preceding question, we are not prepared to respond at this time.

QUESTIONS RELATING TO INDUSTRY'S ROLE IN PROMOTING INTERNET SECURITY

*Question 1.* What is the appropriate role of industry in assuring the security and privacy of Internet users? Should they take the lead?

Answer 1. We believe the role of industry must be one of partnership with users and the government. As in most other areas of commerce, users need to protect

themselves to the extent knowledge and tools are available to them. At the same time, industry's part of the equation is also crucial—Internet businesses and sites must provide secure storage mechanisms for user data, and should affirmatively disclose their privacy practices and policies, whether in the commercial or non-commercial sectors. Industry has also been active in creating and bringing to market new technological privacy solutions.

With respect to data security, we believe the market should take the lead in setting standards that provide strong protection from unauthorized use, through an industry-led process that maintains the flexibility and speed to respond to new market conditions and security threats. Government's role should be to encourage such marketplace developments, while making sure the criminal laws are vigorously enforced.

With respect to privacy, we believe industry should take the lead vis-à-vis government. The history of business' response to the privacy issue is a remarkably good one, and the mechanisms currently in place are much more adaptable, flexible, and economical than any federal regulatory scheme would be.

*Question 2.* To what extent is it necessary for industry to involve law enforcement in taking steps to ensure the security and integrity of the Internet? Could the use of encryption devices, for example, in fact frustrate the ability of law enforcement to provide assistance when such assistance is requested by industry or required by law?

Answer 2. As noted in the answer to the preceding question, we believe government enforcement of current laws is essential to the security and integrity of the Internet. Its performance in responding to recent hacking and distributed-denial-of-service attacks has been admirable. However, we caution the Committee in considering any restriction on the use of encryption. While e-businesses would welcome a world in which no cybercriminal could hide his trail through encryption, we would reject a world in which there could be no real anonymity online, a world in which the initiator of a signal, or author of a message, could be revealed to the government at the push of a button regardless of the circumstances. In short, we as a society must be prepared to strike careful balances in our dual aims to protect the privacy of law abiding users and to enforce the law effectively.

QUESTIONS ON WHETHER GOVERNMENT REGULATION WOULD STYMIE TECHNOLOGIC INNOVATION

*Question 1.* A primary criticism of government regulation of privacy on the Internet is that it would stymie technologic innovation of this industry. Do you agree with this criticism? If you do agree, please describe how this might occur.

Answer 1. Clearly any regulation of business practices changes the future development of the affected economic sector. The impact is most significant, and unpredictable, where, as with the Internet, a true paradigm shift is underway that is changing the way individuals interact with each other and with every kind of institution in our society. In such an environment, it is impossible to prevent even well-meaning government regulation from generating unintended consequences, and many of them may be unproductive or harmful.

Turning specifically to privacy, we believe government's role to date—publicly and privately encouraging and facilitating voluntary, industry-led, privacy programs—has been helpful. Perhaps more importantly, privacy has spurred industry innovation to the public's benefit: business models and technological systems (eg., P3P, the Platform for Privacy Preferences, which will allow privacy preferences to be built into users' browsers) have been crafted to offer the public and businesses different ways of ordering their relationships. These may well be undercut by ill-considered legislation, with the result that the public will have fewer choices rather than more.

Looking backward can illustrate the hazard even of general regulation: can we say with any confidence that the P3P initiative would have reached its current level of development if online privacy had been forced into a simple on-off model five years ago? How then can we have confidence that similar steps today will not undercut the beneficial advances of tomorrow? Though the analogy is not perfect, if everyone is required to wear a gray tunic, tailors go out of business, along with designers, retailers, clothmakers and dyemakers.

*Question 2.* In addition, is it your opinion that any government action would hurt technologic innovation? What actions can the government take to both encourage technologic innovation and address the issue of consumer privacy on the Internet?

Answer 2. In general, government facilitates innovation by providing a stable legal and physical infrastructure, educational opportunity, general conditions for prosperity, etc., while leaving unfettered the imagination and drives of individuals and companies. This implies a balance—some restriction on individual action is nec-

essary to an orderly society. As history tells us, the degree of any regulation obviously must be carefully crafted according to the particular area of activity and the interests affected. In the area of online privacy, we reiterate our position that industry should take the lead, and that any governmental approach must intrude as little as possible into a largely successful industry response.

QUESTIONS ON WHETHER CONSUMER INFORMATION CAN BE USED WITHOUT COMPROMISING ANONYMITY AND PRIVACY

*Question 1a.* Given what an important resource the Internet is for companies to target potential consumer groups, are there ways a consumer's personal information could be made available to third parties for business purposes while still maintaining a consumer's anonymity and privacy?

Answer 1a. Yes. Though this field is new, a few approaches have already been developed. An example is the use of agent-intermediaries: businesses in possession of personally identifiable information can agree to route targeted marketing to individual email addresses based on criteria specified by the marketer without revealing the addresses to the marketer. Similarly, consumers can contract with third party agents for a new online identity through which they can share demographic and other data with marketers while at the same time maintaining the privacy of their email address or other key identifiers. In the same way, it is becoming possible for consumers to make purchases and transfer funds through an intermediary, without revealing their identity to the seller.

*Question 1b.* Can the government take any actions that might help industry do this? If so, what?

Answer 1b. We will be glad to give this some thought. In general we have not been able to adequately address it in the context of the abbreviated time for answering these questions.

QUESTIONS ON WHETHER PRIVACY CONCERNS ARE JUSTIFIED

*Question 1.* National polls indicate that personal privacy is an increasing concern amongst consumers as the Internet is being used more and more each day to conduct personal business such as purchasing consumer goods, banking, and trading.

a. In your view are such privacy concerns justified?

Answer 1a. Certainly both the increasing use of the Internet for sensitive transactions, as well as the growing knowledge and sophistication of Internet users, is causing more and more of us to pay attention to privacy issues. This is a positive development, since it inevitably leads to more prudent behavior.

Industry recognizes online privacy as a key issue and voluntarily is taking unprecedented and ongoing steps to improve privacy policies and practices online. In terms of justification, however, we do feel there has been something of an overreaction. There is no evidence that consumers in their daily online transactions are being routinely victimized by sharing personal information. Indeed, the data indicates consumers should feel more concerned about punching their calling card numbers into a pay phone in an airport, or giving their credit card numbers to a restaurant waiter, or engaging in other offline transactions with which we have come to feel comfortable as a society.

*Question 1b.* Will commerce on the Internet reach its full potential if such concerns are not adequately addressed?

Answer 1b. No, we concur with Committee members and many thoughtful observers that consumers must feel confident about the security of their personal data online, and about the collection and use of personally identifiable information, if the public trust and confidence is to be built which will maximize the Internet's potential benefits to society. The choice, of course, is among various approaches to building that trust and confidence while preserving the unique, and in many cases, as yet undetermined, benefits the new medium can offer.

QUESTIONS ON WHETHER PRIVACY PROTECTIONS DIFFER BETWEEN ON-LINE CONSUMERS AND ON-LINE BUSINESSES

*Question 1.* In the analog world there are different expectations of privacy in different contexts. For example, there is a substantial difference in privacy expectations between the shopkeeper and the shopper. Certainly a consumer would expect to be able to shop for a computer without surrendering significant personal information. But one does expect to have access to sufficient information about the seller to verify that it is a reputable dealer. Such information may be even more important in the virtual world where certain unscrupulous shopkeepers can hide behind technologically-rich facades that give them an aura of credibility.

Does this not suggest we protect the privacy of online shoppers and web surfers, and require disclosure from web site proprietors, especially those engaged in e-commerce; or at least that we should treat differently the privacy claims of people surfing the net and those holding themselves out on the net by opening web sites?

Answer 1. Given the context of the opening paragraph of this question, we are uncertain whether it asks about disclosure of identity, contact information, or other basic information by web site proprietors, or whether it focuses on privacy disclosures. The former concerns a set of issues we have not yet joined with the Committee. We would be glad to respond if the question could be clarified.

---

CENTER FOR DEMOCRACY AND TECHNOLOGY,
*Washington, DC, June 27, 2000.*

Re May 25, 2000 hearing—responses to written questions.

Hon. ORRIN G. HATCH,
*Chairman, Senate Judiciary Committee,*
*Washington, DC.*

DEAR CHAIRMAN HATCH: We are pleased to submit the following responses to follow-up questions stemming from the May 25 hearing on Internet security and privacy.

RESPONSES OF JAMES X. DEMPSEY TO QUESTIONS FROM SENATOR HATCH

QUESTIONS RELATING TO INDUSTRY'S ROLE IN PROMOTING INTERNET SECURITY

*Question 1.* What is the appropriate role of industry in assuring the security and privacy of Internet users? Should they take the lead?

Answer 1. Industry should take the lead on security. The problem of Internet security is not one primarily within the control of the federal government. Particularly, it is not a problem to be solved through the criminal justice system. Internet security is primarily a matter for the private sector, which has built this amazing system in such a short time without government interference. It is clear that the private sector is stepping up its security efforts, with an effectiveness that the government could never match, given the rapid pace of technology change and the decentralized nature of the medium. Indeed, government intervention to protect security through standards or design mandates would be counterproductive and would undermine, not bolster, user confidence.

In contrast, in terms of ensuring consumer data privacy, the Internet requires a multifaceted approach that draws upon the strengths of technology, self-regulation, and legislation to deliver to the American public the ability to exercise control over their personal information. Consistency is critical to consumers, businesses, and the character of the Internet. It is impossible to develop a consistent standard for privacy without legislation. While self-regulatory efforts, auditing, and self-enforcement schemes work for some businesses, on its own these will result in an inconsistent framework of privacy protection. Bad actors will not self regulate: the clueless or new on the scene may not have the resources or where-with-all to participate in regulating their own behavior. Law is critical to spreading the word and ensuring widespread compliance with fair, privacy protective standards. By building a system of self-regulation and legislation, we can create a framework of privacy and instill consumer trust.

Internet privacy legislation can and should support self-regulation and technical developments. The tired debate over self-regulation versus legislation does not serve our mutual interest in privacy protection. It is our collective task to develop a legislative privacy proposal that fosters that best industry has to offer through self-enforcement and privacy enhancing tools. Realizing privacy on the Internet demands that we develop a cohesive framework that builds upon the best all three of these important tools offer.

Finally, to protect against government intrusions on privacy, there is a role for industry and for legislation. Industry should consciously design systems to minimize the collection and retention of personally identifiable information in formats that allow it to be retrieved by the government without the knowledge or cooperation of the record subject. Secondly, legislation is needed to establish strong protections limiting government access to information that is collected.

*Question 2.* To what extent is it necessary for industry to involve law enforcement in taking steps to ensure the security and integrity of the Internet? Could the use of encryption devices, for example, in fact frustrate the ability of law enforcement

to provide assistance when such assistance is requested by industry or required under law?

Answer 2. There is a very limited role for government in ensuring the security and integrity of the Internet. Obviously, attacks on computer systems are crimes and should be investigated and prosecuted by well-trained law enforcement personnel. The Internet industry has demonstrated its willingness to cooperate in properly-focused investigations. In fact, in many computer crime cases, key leads and evidence were voluntarily provided to the government by the private sector.

The Congress need not be concerned that private sector security measures will impede law enforcement investigations, for, on balance, sound computer security measures will prevent far more crime than they will shield or facilitate. Encryption is a perfect example. While the widespread availability and use of strong encryption means that some criminal communications previously accessible to the government will no longer be available, the use of encryption on credit card numbers, proprietary data and other valuable information in transit and storage will prevent far more crime. Similarly, anonymity online, while it shields some criminal conduct, also allows honest individuals to conduct certain activities in unidentifiable ways, reducing the risk of cyber-stalking and identity theft. Government efforts to reduce or eliminate the degree of relative anonymity currently available online could well backfire, just as other government efforts to dictate the design of systems to facilitate government surveillance or access to information are likely to introduce security vulnerabilities that will be exploited by criminals.

QUESTIONS ON WHETHER GOVERNMENT REGULATION WOULD STYMIE TECHNOLOGIC INNOVATION

*Question 1.* A primary criticism of government regulation of privacy on the Internet is that it would stymie technologic innovation of this industry. Do you agree with this criticism? If you do agree, please describe how this might occur.

Answer 1. We do not agree with this criticism as a general matter. Government regulation of privacy need not stymie technologic innovation. To the contrary, government regulation, if done properly, could increase consumer confidence and boost the demand for new online services and computer/telecommunications products.

*Question 2.* In addition, is it your opinion that any government action would hurt technologic innovation? What actions can the government take to both encourage technologic innovation and address the issue of consumer privacy on the Internet?

Answer 2. It would certainly hurt technologic innovation if the government were to mandate design requirements for security, and especially if the government were to require features intended to facilitate government surveillance. The experience under the Communications Assistance for Law Enforcement Act (CALEA) has been very negative. The federal government's decades' long effort to control the availability of strong encryption is another example of the harm that government regulation can do to privacy, security and technologic innovation.

QUESTIONS ON WHETHER CONSUMER INFORMATION CAN BE USED WITHOUT COMPROMISING ANONYMITY AND PRIVACY

*Question 1.* Given what an important resource the Internet is for companies to target potential consumer groups, are there ways a consumer's personal information could be made available to third parties for business purposes while still maintaining a consumer's anonymity and privacy?

Can the government take any actions that might help industry do this? If so, what?

Answer 1. Yes, there are ways a consumer's personal information could be made available to third parties while still maintaining a consumer's anonymity and privacy, but there is little that the government could do to promote these developments short of enacting baseline legislation embodying enforceable fair information practices, as discussed above.

The private sector (corporations, public interest organizations, and standards bodies) must take the lead in developing specifications, standards and products that protect privacy. A privacy-enhancing architecture must incorporate, in its design and function, individuals' expectations of privacy. For example, a privacy-protective architecture would provide individuals the ability to "walk" through the digital world, browse, and even purchase without disclosing information about their identity, thereby preserving their autonomy and ensuring the expectations of privacy.

For example, the Internet Engineering Task Force (IETF) is working on two standards that would create new guidelines for the appropriate use of cookies. While cookies are helpful for Web sites looking to maintain relationships with visitors, they have been implemented in ways that give users very little control and have

been used by some to subvert consumers' privacy. On most browsers, users are given only the option to either accept or reject all cookies or to be repeatedly bombarded with messages asking if it is OK to place a cookie. The IETF is considering two complementary "Internet drafts" that would encourage software makers to design cookies in ways that give users more control. These drafts lay out guidelines for the use of cookies, suggesting that programmers should make sure that:

—the user is aware that a cookies is being maintained and consents to it;

—the user has the ability to delete cookies associated with a Web visit at any time;

—the information obtained through the cookie about the user is not disclosed to other parties without the user's explicit consent; and

—cookie information itself cannot contain sensitive information and cannot be used to obtain sensitive information that is not otherwise available to an eavesdropper.

The drafts say that cookies should not be used to leak information to third parties nor as a means of authentication. Both are common practices today.

QUESTIONS ON WHETHER PRIVACY CONCERNS ARE JUSTIFIED

*Question 1.* National polls indicate that personal privacy is an increasing concern amongst consumers as the Internet is being used more and more each day to conduct personal business such as purchasing consumer goods, banking, and trading.

In your view, are such privacy concerns justified?

Will commerce on the Internet reach its full potential if such concerns are not adequately addressed?

Answer 1. In CDT's view, consumer privacy concerns are indeed justified. We have long stated that the Internet will never reach its potential if such concerns are not adequately addressed. Over the past twelve months privacy concerns surrounding the use of technology to track and profile individuals' has taken center stage. From the joint FTC and Department of Commerce workshop on Online Profiling, to the massive online consumer protest of Doubleclick's withdrawn proposal to tie online profiles to individuals' offline identities, to the private law suits against Realnetworks, to state Attorneys' General actions against Doubleclick—it is clear that policy-makers and the public are concerned with the use of technology to undermine privacy expectations.

There is reason for concern. Third-party cookies, as the FTC Web sweep reports, are routinely found at commercial Web sites. In fact, consumers visiting 78% of the 100 most popular Web sites will be confronted with cookies from entities other than the Web site. While the growth of third-party cookies continues, less than 51% of the top 100 sites that set third-party cookies tell consumers about this practice.

Similarly, the use of "web bugs" or clear gifts—invisble tags that Internet marketing companies use to track the travels of Internet users—has grown exponentially over the past year. Richard Smith, a well-known computer security expert, in his presentation to the Congressional Privacy Caucus stated that in January 2000 approximately 2000 "web bugs" were in use on the Web (according to a search using Alta Vista), but in just 5 months that number multiplied ten-fold to 27,000.

QUESTIONS ON WHETHER PRIVACY PROTECTIONS DIFFER BETWEEN ON-LINE CONSUMERS AND ON-LINE BUSINESS

*Question 1.* In the analog world there are different expectations of privacy in different contexts. For example, there is a substantial difference in privacy expectations between the shopkeeper and the shopper. Certainly a consumer would expect to be able to shop for a computer without surrendering significant personal information. But one does expect to have access to sufficient information about the seller to verify that it is a reputable dealer. Such information may be even more important in the virtual world where certain unscrupulous shopkeepers can hide behind technologically-rich facades that given them an aura of credibility.

Does this not suggest we protect privacy of online shoppers and web surfers, and require disclosure from web site proprietors, especially those engaged in e-commerce, or at least that we should treat differently the privacy claims of people surfing the net and those holding themselves out on the net by opening web sites?

Answer 1. We hesitate to support any requirements of disclosure from Web site operators. The principle of caveat emptor (buyer beware) applies on the Internet with even more force than it does off-line. While the government should prosecute fraud online just as it does fraud offline (we note that the Justice Department has recently created an online complaint system for consumers who suspect they have been the victims of online fraud), we believe that disclosure requirements would be unworkable and ineffective. There is already a tremendous amount of information

available online. Users need to take advantage of the information that is there, not depend on some regulatory mechanism to certify what is reliable and what isn't.

---

RESPONSES OF JAMES X. DEMPSEY TO QUESTIONS FROM SENATOR LEAHY

*Question 1.* Do you support or endorse S. 2448? Are you aware of any companies or organizations that support or endorse S. 2448?

Answer 1. CDT does not support S. 2448 as introduced. We are not aware of any companies or organizations that endorse the bill.

*Question 2.* Please comment on your views of S. 2448 and explain any specific concerns you may have about this legislation.

Answer 2. Our views on S. 2448 are set forth in detail in our testimony and in the attached letter to Chairman Hatch identifying specific areas of concern and making specific suggestions for changes in the bill.

*Question 3.* In my opening statement, I gave the example of the college student who without authorization accesses his professor's computer to see what grade he is going to get and accidentally deletes a file or a message. That conduct may be cause for discipline at the college but would not be a federal crime under current law, unless the conduct caused over $5,000 in damage.

A. Do you think that sort of unethical conduct warrants federal law enforcement attention and should be a federal crime?

Answer 3A. No.

*Question 3. B.* Under S. 2448, this unauthorized access to the professor's computer would constitute a felony violation of 1030(a)(5)(B), punishable by up to 3 years' imprisonment, with a mandatory minimum of at least 6 months in jail, or a misdemeanor violation of 1030(a)(5)(C). Rather than trust federal prosecutors to exercise their discretion to decline such a case, would it be preferable for Congress to define clearly what would and should not be a federal crime?

Answer 3B. CDT does not take a position on mandatory minimum sentences.

*Question 4.* Some have suggested that some change to the Freedom of Information Act (FOIA) would be useful to encourage private sector cooperation with the government in protecting critical infrastructures. I have long supported the FOIA as a critical tool for all Americans to find out what their government is doing. This is healthy and necessary for our democracy. Consequently, I am concerned about proposals that allow agencies to keep "secret" broad categories of records in their possession that may be related to the "critical infrastructure" and to block FOIA requests, with no other justification and no judicial review. This would certainly reduce the FOIA workload of Federal agencies, but labeling information as related to "critical infrastructure" as a means of exempting entire categories of information from the FOIA would, in my view, undercut and pose a threat to the effectiveness of the FOIA.

A. Would you agree with me that any change to the FOIA must avoid undercutting the usefulness of the FOIA and ensure the effectiveness of judicial review?

Answer 4A. Absolutely. CDT supports and applauds the position of Senator Leahy, who has long been a champion for the FOIA and its vital role in our democratic system of open and accountable government. We share Sen. Leahy's concerns about the dangers posed by further FOIA exemptions, particularly if they are drawn in broad terms. If cyber-security is to become a government priority, then information about cyber-security issues in the hands of the government should be subject to public access, to ensure that the government is doing its job, subject only to the narrow national security, law enforcement and proprietary information exceptions of FOIA.

*Question 4B.* What suggestions, if any, do you have for refining the FOIA in ways that would narrowly address the legitimate concerns of the private sector about sharing information to protect our critical infrastructures while at the same time maintaining the presumption in FOIA that federal agency records are subject to the disclosure and that agency actions is subject to judicial review?

Answer 4B. We believe that, if any change is adopted, it would be best to work within the existing framework of the (b)(4) proprietary information exemption to FOIA. The Y2K Information and Readiness Disclosure Act, Pub. L. 105–271, exempted certain Y2K-related information within the context of (b)(4). In other respects, however, the Y2K legislation is not an appropriate model for legislation regarding cyber-security information. CDT has prepared a detailed analysis of one such proposal, H.R. 4246, introduced by Reps. Davis and Moran. A copy of our analysis is enclosed.

* * * * * * *

Mr. Chairman, CDT looks forward to continuing to work with you, with the ranking Senator and with all the members of the Senate Judiciary Committee to craft a focused bill improving privacy and cyber-security. We would be happy to provide to you any further information or assistance we can.

Respectfully,

JAMES X. DEMPSEY, *senior staff counsel.*

---

CENTER FOR DEMOCRACY AND TECHNOLOGY,
*Washington, DC, June 7, 2000.*

Re S. 2448, Internet Integrity and Critical Infrastructure Protection Act of 2000.

Hon. ORRIN G. HATCH,
*Chairman, Senate Judiciary Committee,*
*Washington, DC.*

DEAR CHAIRMAN HATCH: We are pleased to share with you some further specific comments on your bill, S. 2448. We have been grateful, for the attention that you and your staff have shown to privacy concerns. In particular, your staff has spent many hours with us going over the bill both before and after introduction.

*Title I*

We are concerned that Section 101(b)(3) of S. 2448 would amend the federal Computer Fraud and Abuse Act, 18 USC 1030, to make the most trival forms of unauthorized computer access a potential federal crime, by eliminating the $5,000 threshold that currently defines "damage" in the absence of other specific harms.

The $5,000 threshold is important to the purport of § 1030 because otherwise the scope of the statute is exceedingly broad. It was hard for drafters of § 1030 to specify what kinds of conduct should constitute a computer crime. Consequently, subsection (a)(5)(A) is very general: it makes it a crime to knowingly cause the transmission of "information" and as a result intentionally cause damage without authorization to any computer connected to the Internet. Under subsection (e)(8), damage is defined as "any impairment to the . . . availability of . . . a system." Sending a single email to someone who didn't want it impairs the availability of that person's system for the tiny amount of time it takes to download the message, and every user who sends a message to someone who didn't want it intentionally "impairs" the availability of that person's computer for that very short period of time. On the other hand, sending many thousands and thousands of unwanted messages to a system also impairs the availability of that system, but in a way that should be treated as a criminal attack. To make it clear that the latter was a crime but the former was not, § 1030(a)(5) has a damage requirement and damage was defined in terms of a $5,000 Threshold. (In contract, subsections (a)(1)–(4) and (6)(7) of § 1030 do not have damage requirements, because the crimes there are more precisely defined.)

We oppose the elimination of the $5,000 threshold. It will open up a wide range of common conduct to the threat of criminal prosecution. We are especially concerned that the authority would be used selectively and could be used to intimidate those who use the Internet for political advocacy. The concerns are compounded by the other sections of S. 2448 that would require forefeiture to the government of the real and personal property of any person convicted of any violation of § 1030 as expanded by section 101 an expand wiretap authority by making all subsections of § 1030 crimes a predicate for wiretaps.

Indepndently, we are concerned about the implications of forfeiture of real property "used . . . to facilitate" the commission of an offense under § 1030.

Suggested changes: On page 7, we would urge you to strike lines 1 through 5.

On page 9, lines 15 and 16, strike "in any property, whether real or personal," and insert "in any computer equipment."

On page 10, line 11, strike "Any property, whether real or personal," and insert "Any computer equipment".

*Section 302—Satellite TV subscriber privacy*

We commend you for including Sec. 302, which would prohibit satellite TV service providers from disclosing information about their customers and their viewing habits unless the customers have affirmatively agreed ("opted-in") to such sharing. This provision extends to satellite TV viewers some of the privacy protections accorded to cable TV viewers under 47 USC 551. However, S. 2448 is not as strong as the Cable Act: S. 2448 allows disclosure to the government without notice to the subscriber and an opportunity to object, and sets a lower relevance standard for government access, thereby giving satellite TV viewers less protection than existing federal

law affords to cable TV subscribers. We recommend extending all of the privacy protections of the Cable Act to satellite.

Suggested change: On page 31, strike lines 6 through 14 and insert" (I) if the law enforcement agency shows that there is clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case, and (II) if the subject of the information is afforded the opportunity to appear and contest such entity's claim."

*Title IV—FBI/DOJ authority*

CDT endorses the comments of Americans for Computer Privacy, of which we are a member. For the sake of completeness, we restate their comments here.

We are concerned that language in Section 402, specifically 402(a)(4), could be interpreted as giving the FBI the ability (if not the express authority) to set standards for the computer and telecommunications industry. We think subsection (a)(4) unintentionally yet mistakenly gives such authority. Subsection (a)(5) gives NIPC the authority to pursue any mission it wishes.

Suggested change: We strongly urges you to eliminate (a)(4)–(5) altogether and list only the first three purposes, all of which help delineate an appropriate role for law enforcement.

We share ACP's concerns with a couple of the duties listed for the new DAAG created in Section 401. In particular, please note those sections that would become Sec. 507a(c)(2) and Sec 507a(c)(6). The first provision grants the DAAG the power to "coordinate national and international activities relating to combatting computer crime." This grant of authority is too broad. For example, dictating design standards or compelling hacker information from companies both represent "activities relating to combatting computer crime," but the DAAG should not be given authority—implied or otherwise—to carry out these activities.

Suggested change: To address this problem, we suggest that, after "international," the words "law enforcement" be inserted.

*International assistance*

Section 502 permits the Attorney General to disclose information regarding the activities of U.S. citizens or companies to foreign law enforcement authorities, even where the activities are legal under U.S. law. Section 503(b)(2) of S. 2448 permits the US Attorney General to provide computer crime evidence to foreign law enforcement authorities "without regard to whether the conduct investigated violates any Federal computer crime law."

Suggested change: To make it clear that this Title does not expand the Justice Department's investigative authority to investigate lawful conduct in the US at the request of foreign governments, strike section 503(b)(2), lines 17 through 23 on page 54.

*Possible amendments*

We congratulate you on keeping S. 2448 narrow, while at the same time addressing a range of cyber-crime and e-commerce issues. We remain concerned about potential amendments that would introduce new issues, for which CDT and other interested parties would not have had an opportunity to review language and strive for consensus. We stress, as we did in our testimony, that it is important to proceed cautiously, as you have, and keep the bill from becoming laden with other issues that have not been adequately reviewed and refined.

*Pen registers for the Internet*

Primary among the issues we have feared might be offered as amendments to S. 2448 is S. 2092, which the Justice Department is urging be added to S. 2448.

S. 2092 would extend government surveillance authority over the Internet in broad and ill-defined ways. It does so with very broad terminology, stating that the pen register can collect "dialing, routing, addressing or signaling information," without further definition. S. 2092 also would give every federal pen register and trap and trace order nationwide effect, without limit and without requiring the government to make a showing of need, creating a sort of "roving pen register."

We have shared our concerns with Senator Schumer and are committed to working with him to improve his bill. At this point, we understand that Sen. Schumer does not intend to offer his bill as an amendment to S. 2448. A copy of our comments and suggestions on S. 2092 is enclosed.

Again, we thank you for the care with which you have approached these difficult issues and for your willingness to make changes to your bill to accommodate the privacy and civil liberties concerns. We look forward to continuing to work with you to develop a consensus bill that can enjoy widespread support.

Sincerely,

JAMES X. DEMPSEY, *senior staff counsel.*

Enclosure.

CENTER FOR DEMOCRACY AND TECHNOLOGY

AMENDING THE PEN REGISTER AND TRAP AND TRACE STATUTE IN RESPONSE TO RECENT INTERNET DENIAL OF SERVICE ATTACKS—AND TO ESTABLISH MEANINGFUL PRIVACY PROTECTIONS

Pen registers are surveillance devices that capture the phone numbers dialed on outgoing telephone calls; trap and trace devices capture the numbers identifying incoming calls. They are not supposed to reveal the content of communications. They are not even supposed to identify the parties to a communication or whether a call was connected, only that one phone dialed another phone. Nonetheless, in an increasingly connected world, a recording of every telephone number dialed and the source of every call received can provide a very complete picture—a profile—of a person's associations, habits, contacts, interests and activities. For that reason, pen registers and trap and trace devices are very helpful to law enforcement and pose significant privacy concerns. Much of the current debate over surveillance standards relates to the collection of transactional data by these devices and by other means.

A 1986 federal law requires a court order for use of such devices, but the standard for approval is so low as to be nearly worthless—a prosecutor does not have to justify the request and judges are required to approve every request.

These orders apply to email and other Internet activity, but it is not clear what is the Internet equivalent of the dialing information that must be disclosed. In crucial respects, Internet addressing information can be far more revealing than telephone dialing information—not only doesit reveal the precise parties who are communicating, but it can even reveal the meaning or content of communications.

Federal law enforcement agencies conduct roughly 10 times as many pen register and trap and trace surveillances as they do wiretaps. In 1996, the Justice Department components alone obtained 4,569 pen register and trap and trace orders. Most orders covered more than one line: in 1996, 10,520 lines were surveilled by pen registers or trap and trace devices. So much information is collected that Justice Department agencies have developed several generations of computer tools to enhance the analysis and linking of transactional data from pen registers and trap and trace devices.

In response to a Justice Department proposal, legislation has been introduced to authorize judges in one jurisdiction to issue pen register and trap and trace orders to service providers anywhere in the country. S. 2092. Other provisions in the bill could have the effect of greatly expanding the scope of these supposedly limited surveillance devices, allowing the collection of more personally revealing information and imposing expensive burdens on ISPs, portals, and other service providers.

Before the geographic reach of pen register and trap and trace orders is expanded, the privacy standards in the current law should be updated: some real substance should be put into the standard for issuing those orders and the scope of information they collect should be carefully limited.

*The framework of the electronic surveillance laws*

There are three major laws setting privacy standards for government interception of communications and access to subscriber information:

- The federal wiretap statute ("Title III"), 18 USC 2510 et seq., which requires a probable cause order from a judge for real-time interception of the content of voice and data communications. This legal standard is high.
- The Electronic Communications Privacy Act of 1986 ("ECPA"), 18 USC 2701 et seq., setting standards for access to stored email and other electronic communications and to transactional records (subscriber identifying information, logs, toll records). The standard for access to the contents of email is relatively high; the standards for access to transactional data are low.
- The pen register and trap and trace statute, enacted as part of ECPA, 18 USC 3121 et seq., governing real-time interception of "the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." The standard is that of a rubber stamp.

Title III governs the interception of the "contents" of communications, which the statute defines as "any information concerning the substance, purport, or meaning of that communication." 18 USC § 2510(8). Since the Supreme Court has held that the content of communications is fully protected by the Fourth Amendment's limitations on searches and seizures, Title III imposes strict limitations on the ability of

law enforcement to obtain call content-limitations that embody, and in some respects go beyond, the protections guaranteed by the Fourth Amendment. A law enforcement agency may intercept content only pursuant to a court order issued upon findings of probable cause to believe that an individual is committing one of a list of specifically enumerated crimes, that communications concerning the specified offense will be intercepted, and that the pertinent facilities are commonly used by the alleged offender or are being used in connection with the offense. 18 USC § 2518(3).

On the other hand, the Supreme Court has held that there is no constitutionally-protected privacy interest in the numbers one dials to initiate a telephone call. *Smith* v. *Maryland*, 442 U.S. 735, 742 (1979). Accordingly, the pen register and trap and trace provisions in 18 USC § 3121 et seq. establish minimum standards for court-approved law enforcement access to the "electronic or other impulses" that identify "the numbers dialed" for outgoing calls and "the originating number" for incoming calls. 18 U.S.C. §§ 3127(3)–(4). To obtain such an order, the government need merely certify that "the information likely to be obtained is relevant to an ongoing criminal investigation" 18 USC §§ 3122–23. (There is no constitutional or statutory threshold for opening a criminal investigation.)

The Supreme Court has stressed how limited is the information collected by pen registers. "Neither the purport of any communication between the caller and the recipient of the call, *their identities,* nor whether the call was even completed is disclosed by pen register." *United States* v. *New York Tel, Co.*, 434 U.S. 159, 167 (1977) (emphasis added). Recent court decisions have reemphasized that such devices' *"only capability* is ti intercept" the telephone numbers a person calls. *Brown* v. *Waddell,* 50 F.3d 285, 292 (4th Cir. 1995) (emphasis added).

The pen register/trap and trace statute lacks many of the privacy protections found in the wiretap law. Not only is the standard for judicial approval so low as to be meaningless, the government can use pen register evidence even if it is intercepted without complying with the law's minimal provisions: Unlike the wiretap statute, which has a statutory exclusion rule, the pen register/trap and trace law has no such provision, and the Fourth Amendment's exclusionary rule does not apply. There is little chance of after-the-fact oversight, since innocent citizens are unlikely to find out about abuses of the statute: Unlike the wiretap law, the pen register/trap and trace statute has no provision requiring notice to persons whose communications activities have been surveilled. Nor, in contrast to the wiretap law is there any provision for judicial supervision of the conduct of pen registers: Judges are never informed of the progress or success of a pen register or trap and trace. There is also no minimization rule: Section 3121(c) requires the government to use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information used in call processing, the FBI has recently admitted that no such technology exists.

*Applying pen registers to the Internet*

The pen register and trap and trace statute was adopted before the Internet was widely available to ordinary citizens. The definition of pen register says that such devices capture only the "numbers dialed or otherwise transmitted" on the telephone line to which the device is attached. 18 USC 3127(3). The definition of trap and trace device refers to "the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 USC 3127(4).

There are many questions posed by application of the pen register/trap and trace statute to the Internet. The statue almost certainly applies to email and the Web, for it refers to electronic communications. But what are "the numbers dialed or otherwise transmitted"? Can the government serve a pen register order on the ISP or other service provider like Hotmail, to obtain the addresses of all incoming and outgoing emails for a certain account? Does the pen register/trap and trace authority encompass only numbers (Internet protocol addresses) or does it include email addresses or both? Can a pen register or trap and trace order be served on a portal or search engine? What does the statute mean when applied to URLs? Can the government serve a pen register or trap and trace order on CNN and get the address of everybody who has downloaded or viewed a certain article? What information is collected under a pen register order and from whom in the case of a person who is using the Internet for voice communications? What standard applies if the person has DSL or a cable modem?

The importance of these questions is heightened by the fact that transactional or addressing data of electronic communications like email and Web browsing can be much more revealing than telephone numbers dialed.

First, email addresses are more personally revealing than phone numbers because email addresses are unique to individual users. In many offices, while there is only one phone number normally called from the outside, each person has an individual

email address. So while a pen register on a phone line only shows the general number called, a pen register served on an ISP will likely identify the specific recipient of each message. Even in a household, each person online may have a separate email, and may have different email addresses for different purposes, making it more likely that the government can determine precisely who is contacting whom.

Furthermore, if the pen register authority applies to URLs or the names of files transmitted under a file transfer protocol, then the addressing information can actually convey the substance or purport of a communication. If you call (202) 637–9800 on the phone and asks for a copy of our statement on cybercrime and Internet surveilliance, a pen register shows only that you called the general CDT number. If you "visit" our website and read the statement, your computer transmits the URL *http://www.cdt.org/security/000229judiciary.shtml,* which precisely identifies the content of the communication. Does a pen register served on our ISP or our web hosting service require disclosure of that URL? If so, the government has no trouble knowing what you read, for typing in the same URL reveals the whole document.

Such revealing information appears in other addresses:

If you search Yahoo for information about "FBI investigations of computer hacking," the addressing information you send to Yahoo includes your search terms. The URL looks like this: *http://search.yahoo.com/bin/search?p=FBI+and+hacking+investigations.*

If you search AltaVista for "hacker tools," the "addressing" data looks like this: *http://www.altavista.com/cgo-bin/query?pg=q&sc=on&hl=on&q=hacker+tools&kl=XX&stype=stext&search.x= 25&search.y=11.*

If you send a message to Amazon.com to buy a book, this is what the URL looks like: *http://www.amazon.com/exec/obidos/handle-buy-box=0962770523/bookglance/002–9953098–4097847,* where 0962770523 is the standardized international catalogue (ISBN) number of the book you are buying.

Computer security expert Richard Smith has identified numerous ways in which the URLs sent to DoubleClick include personal information about travel plans, health, and other matters. See attached memo and *http://www.tiac.net/users/smiths/privacy/banads.htm.* Can a pen register order be served on DoubleClick? Would it cover the detailed information found in URLs delivered to DoubleClick?

These questions did not exist in 1986, when the pen register statute was enacted. They illustrate how outdated is the rubber-stamp standard of the current law. All of these questions should be addressed before the scope of the pen register statute is further extended.

*Jurisdictional expansion of the pen register/trap and trace statute*

18 USC 3123(a) currently states that a judge shall authorize the installation and use of a pen register or trap and trace device "within the jurisdiction of the court." The Justice Department argues that this jurisdictional limitation (no different than the jurisdictional limitation that applies to search warrants or subpoenas in the "real" world) poses a burden to law enforcement conducting investigations in cyberspace, since a communication may jump from one computer to another.

While there is some apparent logic to the government's argument for tracing computer data across jurisdictional lines, the proposed change would not be limited to computer communications—it would also apply to plain old telephones. Nor would it be limited to situations where it appeared that communications were passing through multiple service providers: it would allow a Miami judge to authorize the use of a pen register in New York on communications starting and ending in New York.

Furthermore, orders issued under the proposed change as introduced would have no limits. A normal subpoena, even one with nationwide effect, is addressed to a specific custodian of the desired information. Fed. R. Crim. Proc. 17(c). This requirement does not appear in S. 209; instead, the government would receive a blank order, which it could presumably serve on multiple, unnamed service providers, with no limit as to time or how often the subpoena could be used.

If the pen register and trap and trace provisions are given nationwide effect, it should not automatically apply to every such order. There should at least be some requirement that the applicant explain to the judge's satisfaction why authority is sought to conduct the investigation across jurisdictional lines: Section 3122(b) should be amended to require in the application, if an order with nationwide effect is sought, a full and complete statement as to the grounds for believing that some of the communications to be identified originate or will terminate outside the jurisdiction of the issuing court or are passing through multiple service providers and that the cooperation of multiple service providers or service providers in other jurisdictions will be necessary to identify their origin or destination. And 3123 should be amended to require the judge to specify to whom the subpoena is directed by

name, as well as the geographic extent of the order and the time within which it is effective. (Limiting language or geographic extent already appears in the statute. 3123(b)(1)(C).)

*Establishing meaning privacy standards for pen registers*

Any territorial extension of the reach of trap and trace or pen register orders should also be coupled with a heightened standard for approval of such devices. Under current law, a court order is required but the judge is a mere rubber stamp—the statute presently says that the judge "shall" approve any application signed by a prosecutor saying that the information sought is relevant to an investigation. Currently, the judge cannot question the claim of relevance, and isn't even provided with an explanation of the reason for the application. Given the obvious importance of this "profiling" information, section 3122(b)(2) should be amended to require the government's application to include a specific description of the ongoing investigation and how the information sought would be relevant and material to such investigation, and section 3123(a) should be amended to state that an order may issue only if the court finds, based on a showing by the government of specific and articulable facts, that the information likely to be obtained by such installation and use is relevant and material to an ongoing criminal investigation.

The second change needed is to define and limit what information is disclosed to the government under a pen register or trap and trace order, especially those served on an Internet service provider or in other packet networks. Unfortunately, S. 2092 goes in the opposite direction. It would amend the definition of pen register devices to include "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." This completely looses the current sense of the statute, which is limited to information identifying the destination of a communication. The phrase "dialing, routing, addressing or signalling information" is very broad. It increases the amount of information that can be ordered disclosed/collected, in ways that are unclear but that are likely to increase the intrusiveness of these devices, which are not supposed to identify the parties to a communication and not even supposed to disclose whether the communication was completed. It goes will beyond merely eliminating the archaic reference to telephone lines.

A much better way to phrase the pen register definition would be: "dialing, routing, addressing or signalling information that identifies the destination of a wire or electronic communication transmitted by the telephone line or other subscriber facility to which such device or process is attached or applied,".

Similarly, the trap and trace definition could be amended to read: "a device or process that captures the dialing, routing, addressing or signalling information that identifies the originating instrument or device from which a wire or electronic communication was transmitted." These amendments should be coupled with statutory language or legislative history making it clear that pen registers do not authorize interception of search terms, URLs identifying certain documents, files or web pages, or other transactional information.

As an oversight matter, it would be useful to include reporting requirements in the pen register statute that are closer to those applicable to wiretaps. Currently, the statute requires only reports for pen registers and trap and trace devices applied for by the Justice Department, so there is no way of knowing what is done by other federal law enforcement agencies or state and local authorities.

Finally, it should be made clear that any changes to the statute do not expand the obligations on carriers under the Communications Assistance of Law Enforcement Act. Currently, a debate is underway over the meaning of CALEA. The government would almost certainly cite S. 2092's amendments to the definitions of pen register and trap and trace device as justification for requiring carriers to install additional surveillance features. It must be made clear, for example, that the pen register/trap and trace statute's reference to identifying the origin of communications does not imply a design mandate for identification or traceability.

For more information, contact: Jim Dempsey (202) 637–9800

# What are banner ads saying about us?

Web Programming > Internet Privacy > Banner ads and personal information

Richard M. Smith (smiths@tiac.net)
Feb. 14, 2000

Most people who use the Internet probably do not realize that banner ads that they are seeing on Web pages are also sending information about them back to Internet marketing companies. In this write-up, I have put together examples of how one of these marketing companies, DoubleClick (http://www.doubleclick.net), is receiving a great deal of sensitive information about people as they surf the Web. I chose to focus on DoubleClick because they are largest provider of banner ads on the Internet. Their servers currently send out more than a billion banner ads every day according to a recent company press release.

I have been tracking over the last couple of months, what information is being sent from my own computer to DoubleClick ad servers. I used a packet sniffer to do the monitoring. I found more than a dozen examples from different Web sites of information being transmitted to DoubleClick that most people who consider rather sensitive. All this information can be tied to me, because all transmissions to the DoubleClick ad servers also include the same unique ID number in a DoubleClick cookie. I found both personally identifiable information and transactional data being sent to DoubleClick servers.

Personal data I saw being sent to DoubleClick servers included:

- My Email address
- My full name
- My mailing address (street, city, state, and Zip code)
- My phone number

Transactional data that was sent to DoubleClick included:

- Names of VHS movies I am interesting in buying
- Details of a plane trip
- Search phrases used at search engines
- Health conditions

In some cases, this information was explicitly being transmitted by Web sites to DoubleClick encoded in the URLs of banner ads. In other cases, the data is encoded in the URLs of the Web page themselves. The Web page URLs are sent to DoubleClick servers as referring URLs when banner ads are fetched.

Except for one banner ad from LifeMinders, all of the data is sent to DoubleClick when I viewed the Web pages. It was not necessary for me to click on the banner ads for information to be sent to DoubleClick servers.

At some Web sites, I found that personal data is accidentally being leaked in referring URLs. I reported these problems to the sites and they have fixed the leaks either by removing the banner ads from Web pages or removing the personal data from URLs.

The following tables provide details of the information I saw going to DoubleClick. Personal data and transactional data is color-coded in the URLs.

## Personal identifable data sent to DoubleClick

AltaVista Yellow Pages -- Complete home address (Fixed January 2000)
**Banner ad URL:** http://live.av.com/scripts/search.dll?ep=7&gca=address&orderby=distance&sstreet=172+mason+terr&scity=brooklin
**Referring URL:** http://ad.doubleclick.net/ad/my.av.com/findanything;sz=468x60;ord=8089440000

RealNetworks -- Registration information (Fixed December 1999)
**Banner ad URL:** http://ad.doubleclick.net/ad/real.networks/banner;sect=download;sz=468x60;ord=4296?
**Referring URL:**
http://proforma.real.com/real/player/player.html?RApromo=&language=English&s=1&dc=161514&src=000103realhome%2Cnav%2C991228

HealthCentral -- Email address
**Banner ad URL:** http://ad.doubleclick.net/adi/www.healthcentral.com/newsletters/main;cat=healthcat=health;;ord=13065
**Referring URL:** http://www.healthcentral.com/newsletters/newsletters.cfm?primaryemail=smiths@tiac.net&NewsLetterType=Specific&S

Amazon/Internet Moive Database (IMDb) -- Birthday
**Banner ad URL:** http://ad.doubleclick.net/ad/www.imdb.com/OnThisDay;p=OnThisDay;sz=468x60;ord=142577
**Referring URL:** http://us.imdb.com/OnThisDay?day=28&month=November

Travelocity -- Email address
**Banner ad URL:** http://m.doubleclick.net/viewad/59705-295964options_old.gif
**Referring URL:** http://dps1.travelocity.com/promoptout.ctl?email=smiths@TIAC.NET

LifeMinders -- Email address
**Banner ad URL:** http://ad.doubleclick.net/click;857127;0-8388608;0;321977;1-468|60;0|0|0;;%3fhttp%3a%2f%2fwww.lifeminders.com/lifeminder30/banner/SignUpDAT.asp?MktgSourceCD=LLQA1943&Email=smiths@tiac.net&image.x=11&image.y=7
**Referring URL:** http://ad.doubleclick.net/adi/altavista.digital.com/result_front;kw=Aureate;cat=stext;ord=3373783

**Transaction information sent to DoubleClick**

AltaVista -- Search string
**Banner ad URL:** http://ad.doubleclick.net/adi/altavista.digital.com/result_front;kw=sports+cars;cat=stext;ord=203730346
**Referring URL:**
http://www.altavista.com/cgi-bin/query?pg=q&sc=on&hl=on&q=sports+cars&kl=XX&stype=stext&search.x=39&search.y=11

Lycos -- Search string
**Banner ad URL:** http://ad.doubleclick.net/ad/ly.ln/r;kw=sports+cars;cat=;sz=468x60;ord=7088991092?
**Referring URL:** http://www.lycos.com/srch/?lpv=1&loc=searchbp&query=sports+cars

Travelocity -- Plane trip information
**Banner ad URL:** http://ad.doubleclick.net/ad/travelocity.TRAVELOCITY.com/aircairline;orig=BOS;dest=LAS
**Referring URL:** http://dps1.travelocity.com:80/logmguest.ctl?SEQ=950480201958005

Buy.com -- Movie title
**Banner ad URL:**
http://ad.doubleclick.net/ad/buy.videos.sm/videos-search;kw=enemy+of+the+state;cat=videos-search;sz=120x90;title=1;num=1234567
**Referring URL:** http://www.buy.com/videos/searchresults.asp?searchtype=1&format=1&qu=enemy+of+the+state

drkoop.com -- Health condition information
**Banner ad URL:** http://ad.doubleclick.net/ad/dr.koop.dart/diabetes;sz=120x60;ord=8702047
**Referring URL:** http://www.drkoop.com/conditions/diabetes/

Amazon/Internet Moive Database (IMDb) -- Movie SKU
**Banner ad URL:** http://ad.doubleclick.net/ad/www.imdb.com/Title;p=Title;sz=468x60;kw=76759;g=Sci;g=Act;g=Adv;ord=145171
**Referring URL:** http://us.imdb.com/Title?0076759

CENTER FOR
DEMOCRACY
and
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 Eye Street, NW Suite 1100
Washington, DC 20006
(202) 637-9800
FAX (202) 637-0968
email: info@cdt.org

May 2000

**Davis-Moran Cyber Security Information Act**
**H.R. 4246**

## CDT Analysis

The bill has four main components: an antitrust exemption, a FOIA exemption, a disclosure and use limitation, and an exemption from the Federal Advisory Committee Act. The first is easily dealt with: The antitrust exemption, Sec. 6 of the bill, is probably as harmless as it is unnecessary, although the Antitrust Division may worry that the exception to the exemption, Sec. 6(b), by being too narrow, creates an implication that the exemption is broader than intended.

The FOIA and disclosure/use issues are far more complicated. They are quite separate issues too: While the FOIA exemption has attracted the most attention, and while the assertion of need for the bill is based on stated concerns that the FOIA will expose to terrorists and hackers vulnerabilities in power grids and other key infrastructures, the disclosure/use limitations are limits on the government and on other businesses. They are very broad and, as drafted, could have many unforeseen consequences, including unintended negative effects on the very companies they are meant to protect.

### What is the national goal: immunity or accountability?

The disclosure and use limitations, which are intended to shield companies from liability exposure based on shared information, seem to run counter to other cyber security initiatives that seek to use the liability/insurance system, auditing standards, and disclosure processes such as those of the SEC to promote accountability and therefore encourage cyber security remedial measures.

### FOIA Issues:

### Is the government the clearinghouse?

Some of the questions posed by H.R. 4246 stem from the fact that it is not clear what model for information-sharing it seeks to promote: will a government agency serve as the information clearinghouse, or will the sharing occur within industry. The sponsors of the bill cite the industry ISAC ("information sharing and analysis center") model. But the financial services industry has created an ISAC without FOIA concerns since the government is not a participant and therefore nothing is subject to FOIA.

### Sharing versus nondisclosure

Whether or not the government is the clearinghouse, the bill's drafting raises a host of questions: The bill says that, except with the express consent or permission of the provider, covered information "shall not be disclosed to or by any third party." Sec. 4(c)(2). This basically gives the submitter of the information control over its use and disclosure. Presumably, most submitters would specify that the information could be

disclosed to other members of a trusted network. The bill doesn't say who will decide who is in and who is outside that network. With respect to vulnerabilities in widely-used computer systems, limiting disclosure to a small network poses a risk that the information will not get to all those who would benefit from it. It is one thing for industry to form sectoral or regional sharing systems - it is different to enshrine non-disclosure as a Federal legal mandate.

A "submitter controls" approach has appeal, but it poses some problems. What if information is submitted anonymously, so that the recipient (governmental or not) cannot go back and seek permission to disclose? This would mean that the recipient would be prohibited from disclosing this information even to the intended target of an attack. Similarly, if the information comes from an informant, who said he didn't want it disclosed, again the government would be precluded from overriding the desire of the informant, even to the extent of sharing the information with the intended target.

Could the nondisclosure and nonuse provisions prevent companies from defending themselves against false accusations? If a claim is made that Windows has a vulnerability, doesn't Microsoft deserve to know that somebody is claiming that its product is faulty? Shouldn't the government be able to share that allegation with Microsoft and get Microsoft's response? Yet under the bill, if the submitter of vulnerability information gives consent to share it with anybody except Microsoft, that restriction controls.

If the allegation is untrue, shouldn't Microsoft be able to seek remedies against the person who disparaged its product? The civil litigation prohibition restricts Microsoft and other companies from defending themselves against false allegations.

Do the nondisclosure and nonuse provisions preclude standard contract remedies? For example, if a government vendor admits that one of its systems is insecure, shouldn't the government agency that has a contract to purchase and use the system be able to cancel its contract and defend itself against a breach of contract suit on the ground that the supplier admitted that the system was insecure? Yet Sec. 4(c)(3) says that the information may not be used by any Federal or State entity, agency of authority or by any third party, directly or indirectly, in any civil action arising under any Federal or State law.

**Definitions: What information is covered?**

A very difficult issue is defining what information is covered.

A central term in the bill is "cyber security statement," defined as "any communication ... by a party to another, in any form or medium including ... a website ... concerning the cyber security of that entity." Sec. 3(5). On the one hand, that seems too narrow, since, if the words "of that entity" refer to the party making the statement, the bill would not include a statement by one entity about the cyber security of another entity. Thus, if a security expert finds a flaw in the system or program of another company, and warns the government, that information is not covered, since it is not a statement about the cyber security of the entity making the communication. Also not covered are in-house assessments that are not communicated "to another." Therefore, if the FAA discovers a vulnerability in its air traffic computers but doesn't tell "another," the information sitting in the FAA files is still subject to FOIA.

Compounding this problem, the bill only covers "cyber statements or other such information provided by a party in response to a special cyber security data gathering request made under this section." This means that any information not communicated "in response to a special cyber security data gathering request" is not covered. Unless every

Federal agency with CIP responsibilities immediately issues a blanket special data gathering request for any and all cyber security information, this will create confusion as FOIA processors try to determine whether cyber security information was obtained in response to a designated request or came into the government's possession independently. This provision may actually curtail disclosure to the government, since companies may hesitate to share cyber security information with agencies that have not issued "special cyber security data gathering requests." Also, the bill doesn't seem to cover information in government files before date of enactment, since it would not be information provided in response to a "special cyber security data gathering request made under this [bill]."

On the other hand, the definitions seem overbroad. They cover "any communication by a party to another ... concerning an assessment ... concerning the cyber security of that entity, its computer systems, its software programs ... or commenting on ... the cyber security thereof." This means that a statement by a Microsoft engineer commenting on a news report about an alleged security flaw in Windows is a covered "cyber security statement." It is subject to the restrictions of the bill "except with the express consent or permission of the provider." Does that mean that one hearing that comment shall not disclose it unless the engineer expressly gave permission to do so?

The bill includes statements posted on cyber security Internet website, a defined term. Sec. 3(4). There are hundreds, perhaps thousands, of such sites in existence now, run by the FBI < http://www.fbi.gov/nipc/nipcaaw.htm>, the CERT at Carnegie-Mellon, Cisco <http://www.cisco.com/warp/public/707/advisory.html>, L0pht <http://www.l0pht.com>, and many others. Attrition.org lists 3027 onsite and offsite security advisories: <http://www.attrition.org/security/advisory/>. There is no reason to cover these and then exempt them under the public disclosure exception of Sec. 4(d)(2). (The exception requires "the express consent of the party." Is that the express consent of the party owning the system to which the information relates, the party making the statement, or the party posting it online?) Anyhow, as pointed out below, the website provision is drawn from the Y2K Act, where it served a very different function. It is inapplicable here.

Any Federal agency may expressly designate a request for information as a "cyber security data gathering request," but the bill goes on to say that a cyber security data gathering request "shall be a request from a private entity ... to a Federal entity." It goes further to say that a cyber security data gathering request "shall be deemed to have been made ... when the Federal entity ... has voluntarily been given cyber security information gathered by a private entity ... including by means of a cyber security Internet website." This seems to say that "a cyber security data gathering request ... shall be deemed to have been made" whenever the government is given information. Is the government "given" information when it is published on a website, printed in the newspaper, sent to a government employee who subscribes to a cybersecurity mailing list, or otherwise provided to the government?

**Is the bill necessary?**

The Justice Department has determined that it could successfully defend against FOIA requests for cyber security information under the (b)(4) FOIA exemption for proprietary information. See Critical Mass Energy Project v. Nuclear Regulatory Commn, 975 F.2d 871, 880 (D.C. Cir. 1992 (en banc), cert denied, 507 U.S. 984 (1993) ("Exemption 4 protects any financial or commercial information provided to the government on a voluntary basis if it is of a kind that the provider would not customarily release to the public."). In some cases, the FOIA exemptions for national security information (b)(1) and law enforcement information (b)(7) would also be available.

But some argue that the bill is necessary to overcome industry reluctance (however unjustified legally) to share information with the government. Yet given the issues raised above, a FOIA exemption and/or a disclosure and liability exclusion could serve to shield information that one party in a business-to-business dispute would want to obtain and use.

**Y2K precedent not applicable**

H.R. 4246 is loosely, but only loosely, patterned on the Y2K Information and Readiness Disclosure Act, Pub. L. 105-271. The Y2K Act addressed such a different problem and from such a different perspective that it is probably not a useful model for the cyber security issue. Y2K involved a known problem that was going to cause unpredictable damage unless fixed. It made no sense to hide the problem out of fear that it could be exploited by terrorists. The main focus of the Y2K Act was liability associated with the disclosure and exchange of Y2K readiness information. FOIA was a minor concern. The goal was not to keep Y2K information secret, but to disclose it, so the public could know whether the problem was being solved.

Compare the purposes section of the Y2K bill ("to promote the free disclosure" of Y2K information and "to assist *consumers*, small businesses and local governments") with the purposes section of H.R. 4246 ("to promote the secure disclosure" of cyber security information and "to assist private industry and the government") (emphasis added). Compare also Sen. Bennett's statement on introduction of the Y2K legislation, where he explained that the Y2K bill "attempts to limit the legal liability of corporations and other organizations who in good faith *openly* share information about computer and technology processing problems and related matters in connection with the transition to the Year 2000." (Emphasis added.) Similarly, lead co-sponsor in the House, Rep. Eshoo, said: "This legislation frees organizations to communicate more openly *with the public* and, just as importantly, with each other, about the status of Year 2000 work on critical systems." (Emphasis added.)

The Y2K bill ended up as a very complicated law of short term duration. There are many details in the Y2K Act missing from H.R. 4246. Most notably, the Y2K Act's FOIA exemption stated that Y2K statements were exempt under (b)(4) of the FOIA, the exemption for proprietary data, while H.R. 4246 contains no reference to (b)(4). A bill that fits within the preexisting framework of exemption (b)(4) is less likely to given an overbroad interpretation than a free-standing or (b)(3) exemption.

For further information, contact Jim Dempsey (202) 637-9800 jdempsey@cdt.org