S. HRG. 106–1057

# THE "CARNIVORE" CONTROVERSY: ELECTRONIC SURVEILLANCE AND PRIVACY IN THE DIGITAL AGE



## HEARING

BEFORE THE

## COMMITTEE ON THE JUDICIARY
## UNITED STATES SENATE

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

SEPTEMBER 6, 2000

**Serial No. J–106–105**

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

74–729 WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (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



## QUESTIONS AND ANSWERS

# THE "CARNIVORE" CONTROVERSY: ELECTRONIC SURVEILLANCE AND PRIVACY IN THE DIGITAL AGE

**WEDNESDAY, SEPTEMBER 6, 2000**

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

The committee met, pursuant to notice, at 10:08 a.m., in room SD–226, Dirksen Senate Office Building, Hon. Orrin G. Hatch, (chairman of the committee) presiding.

Also present: Senators Specter and Leahy.

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

The CHAIRMAN. We are happy to welcome all of you out to today's hearing. The purpose of our hearing today is to examine the effect that new surveillance technologies, such as the FBI's now too famous Carnivore, is having on the important public policy balance between personal privacy rights and law enforcement in the digital age.

That the context of this hearing is important goes without saying. The Internet is rapidly becoming a dominant means by which Americans transact business, receive news and information, communicate with their families, and even have fun. A recent report states that over 40 million Americans are currently using the Internet, and that the rate of increase is nearly 55,000 new users every day. Over three million Web pages were created every day in 1999.

Clearly, the Internet is becoming a pervasive feature of daily life, and the technology on the horizon promises to make it even more so. Additionally, the Internet's ability to allow anyone, regardless of wealth or status or political clout, to share opinions with the world, makes it the ultimate first amendment-enabling technology.

But as with many great technological developments and achievements, the Internet's greatest strength is also its most vulnerable weakness. The huge amounts of data speeding through the Internet, including phone numbers, addresses, credit card numbers and bank account information, have facilitated an online crime wave. And the same ease of use that has motivated so many people to rely on the Internet has also given rise to a new breed of swindlers, vandals and terrorists who are short-circuiting the Internet's benefits by waging denial of service attacks, or who are turning the Internet into a weapon by spreading computer viruses.

Only last week, a 24-year-old California man was charged with securities fraud after a fake news release posted on a Website claimed that the Emulex Company had lost its CEO and would restate its last quarter's earnings to show a loss instead of a profit. The hoax caused a $2 billion loss in the value of this company.

Unfortunately, this is only one of the myriad types of crime committed via the Internet. The use of e-mail has been a boon to criminals engaged in spreading child pornography, coordinating illegal drug rings, stealing intellectual property, and much more. America's Internet users are legitimately concerned that surfing the Internet is like walking in a big city at night: the enjoyment is tempered by a fear of what is lurking unnoticed in the dark alleys. Even short of illegal activity, Americans are concerned about the ability of businesses and other Web site hosts to collect and share personal information, and to track individuals' interests, purchases, and other data.

On the other side of the debate is an equally important concern that the Government should not intrude unduly into commerce and personal lives. Unlike many other governments in the world, the United States does not permit its law enforcement agencies easy access to phone lines, the mail, and other sources of private information.

The computer geniuses who are innovating with new technology and creating e-commerce companies are understandably wary of opening up their hard drives and servers to government data traffic control. And individuals who use the Internet for personal communications, purchases and hobbies are justifiably reluctant to allow an "Orwellian Big Brother" to monitor which Web sites they visit or what messages they send through cyberspace.

In short, America's Internet users want a balanced approach to Internet integrity that guarantees protection of personal privacy, but that allows limited and constitutionally-sanctioned access to law enforcement when necessary for the protection of law-abiding citizens.

Some believe these goals are in hopeless conflict. I personally do not. I firmly believe that properly calibrated laws can simultaneously protect the Internet from criminals and terrorists, respect the privacy interests of all Americans, and allow the Internet to flourish free from burdensome regulation. In fact, I recently introduced a bill, the Internet Integrity and Critical Infrastructure Protection Act of 2000, that strives to do that in certain circumstances.

Although no law could prevent bad actors from misusing the Internet, my bill will provide much needed resources and investigative tools to law enforcement and will update our computer abuse laws to help deter and prevent such activities.

So it is within the context of this debate that we are holding today's hearing to examine the constitutional and policy implications of new surveillance technologies, in general, and the FBI's Carnivore system in particular. I hope we get a better understanding of what Carnivore is and how it operates today. As I understand it, it permits law enforcement agencies to gather specific electronic-mail information, presumably circumscribed by court order, relevant to the commission of a crime.

There has been a lot of controversy surrounding this system, perhaps justified, perhaps not. Much of the controversy and confusion is due to differences in opinion on the degree of protection against improper searches by the Government that the fourth amendment of our Constitution provides each citizen, and whether current laws—which were written before the Internet became the revolutionary force in communications that it has become—need updating in this new digital age. It is this constitutional challenge created by technological advancement that we are here to examine today.

Now, before we hear from today's witnesses, I want to note that the technical questions about Carnivore are to be addressed by a DOJ-commissioned independent technical review. These technical questions include whether the Carnivore system could interfere with the proper functioning of Internet service providers, whether the system might provide investigators with more information than is authorized by a court order, or whether the system's capabilities could give rise to a risk of misuse, leading to improper invasions of privacy. I think this is a very important study which likely will affect some of our policy decisions, and we will examine the report's findings once it is conducted in a future hearing.

With that background, I will introduce our distinguished witnesses as soon as the ranking member makes his comments.

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

Senator LEAHY. Thank you, Mr. Chairman. We talk about ISP's and URL's and all this new language of the Internet age that Mr. Cerf and others gave us. And I thank you most of the time, Mr. Cerf. There are days when connections are slow when I don't, but that is not your fault.

What we are doing here actually is carrying on a 200-year conversation about how we assure the rights of the American people, the rights of all of you, the rights of me and the chairman and everybody else to be secure in their persons, in their houses, in their papers, and their effects, secure against unreasonable searches and seizures. That obviously goes back to the Constitution's Fourth Amendment.

Back at the time of the Framers, you gained access to a person's private effects by being there. You were going to find out what was in somebody's desk drawer by walking in the house and opening the desk. You were going to find out what papers they had in their inside pocket by searching them and searching their inside pocket. It is a lot different today. You can be a mile away or 10,000 miles away and search information about most families, certainly those who have computers and are on the Net.

This is really the concern that I have. On the one hand, I ask the question, are we dealing with a legitimate surveillance tool in a cyber age when we know that criminals can move billions of dollars electronically; when terrorists can plan damage from a point on another continent to a residence or a warehouse in the United States; when a kidnaper can deal with somebody in a different State, or where a child abuser can seek out a victim hundreds of miles away. But on the other hand, is this surveillance something that goes way beyond what we the American people want?

It is legitimate to ask the FBI, which has come up with this unfortunately named device—and I suspect nobody has claimed credit as the author of the name, but we should not allow ourselves to be distracted simply by the name. Call it anything you want. The question we have to ask, and legitimately, is has the FBI given themselves a tool which allows them to go way beyond what the American people would allow, what the stated mandate of the FBI would allow, and certainly what the Congress or anyone else would accept.

I think these are the kinds of questions that we have to ask because new communications technologies both have benefits and pose challenges to privacy and law enforcement. The Congress has, I think, worked successfully, in a bipartisan fashion, to mediate this tension with a combination of very stringent procedures for law enforcement access to our communications, but also legal protections to maintain privacy and confidentiality, whether it is in person, over the telephone, fax, computer, or elsewhere.

In fact, in 1968 the Congress passed comprehensive legislation authorizing Government interception of voice communications over telephones, and so on. We returned to this in 1986, when we passed the Electronic Communications Privacy Act, which I sponsored. That law established procedures for law enforcement access to electronic mail systems, to remote data processing systems, and had privacy safeguards for computer uses. It talked about the way we get pen registers and traps, and so on. These pen register and trap and trace orders, though, were not to be used to identify or record the contents of the communications.

Now, we have this new surveillance tool and we have to find out where it fits in the mix. I understand Carnivore is a surveillance tool, a software program developed by the FBI, installed by the FBI at the physical premise of an Internet service provider, to intercept Internet communications following a court order.

The order may authorize capture of an entire communication or it may be limited to addressing information, sort of like a pen register. This program, though, is versatile enough that the FBI can use the same program to accommodate variations in court order authorizations. So I want to hear more about how it works, the precise kind of information the program produces to the FBI, and what controls the FBI has in place when Carnivore is used to ensure the program is operated only as authorized by the court order.

This is keeping in mind the fact that usually the court orders are going to be designed exactly the way the Government wants them to be. But notwithstanding that—and I am sorry some of the courts may take offense at that, but that is a fact. And notwithstanding that, I want to make sure it still doesn't go beyond it.

Carnivore is not "freeware" available for download and public scrutiny. So somewhere, somebody has got to be able to scrutinize it. I commend the Attorney General for her efforts to address this concern and hiring an independent contractor to conduct a technical review of the surveillance program. It is a constructive step that moves beyond the hypothetical discussions of Carnivore.

Now, there is no dispute that the stringent legal requirements governing wiretaps apply to Carnivore when it is used to capture

the content of e-mails or other computer transmissions. I think all of us here on the Judiciary Committee would agree with that.

There is also no dispute that both the text and the subject line of an e-mail message are content which law enforcement may intercept only under a wiretap order. But we still want to know whether the legal standards for its use are adequate and exactly what it does.

Telephone companies regularly comply with wiretap and other legitimate surveillance orders, as do Internet service providers. But if the Internet service provider doesn't have the capability or willingness to do it, to execute court orders, fine; I will accept the fact that law enforcement can step in. I think Carnivore is for that. But, again, is it limited, and will it limit itself to what a willing ISP would give if they were willing to carry out the order themselves?

Second, Carnivore works by sifting through the Internet traffic of a particular ISP to capture the particular information or communication authorized by a court order. I think privacy advocates are rightly concerned about whether Carnivore accesses too much, not only too much information about Internet users, but also too much information about the communications that are the subject of the court order.

We know that the Internet breaks down communications into separate packets that are reassembled at the destination point. The FBI will say that Carnivore is able to find the different packets that make up a suspected Internet criminal's message only by sifting through all the traffic. Technically, that is correct, but that might not be a great comfort to all the other Internet users who are not subject to the court-ordered surveillance but have their messages being looked at.

It comes down to this: Carnivore is like a car. It can be very useful or it can be abused. You can drive back and forth to take your kids to school or you could have a drunk driver come down the road and wipe out a family. What counts is the rules of the road, but also what counts is what license we give the driver, and I am interested in the license and hearing from the witnesses today whether surveillance rules we developed for the analog telephone environment and for the pre-Internet computer environment are adequate to protect our current expectations of privacy when we go online.

And I must say in that regard, Mr. Chairman, that we have the CALEA Act, which we all worked on very closely and worked closely with the FBI. And in many ways, the FBI has tried to push the envelope way beyond what I as one of the authors of that bill intended and what many of the others did. Because of that, I take a little more careful view of what they might say and whether the FBI now is going to push beyond the envelope of what they are allowed.

In closing, I am a strong proponent of the Internet. I don't know of anybody in the Senate who is a stronger proponent. But I am a defender of our constitutional right to speak freely, and also I have the typical Vermonter's view of privacy that we should keep private our confidential affairs from either private sector snoops or unreasonable government searches. These principles can and must

be respected when law enforcement agencies use surveillance tools to uncover and hold accountable criminal wrongdoers.

So, Mr. Chairman, I think you have an excellent hearing. I think it is a wise one to have. I would put my whole statement in the record so we can hear from the witnesses.

The CHAIRMAN. Well, thank you, Senator, and we will put all statements in the record at this point.

[The prepared statement of Senator Leahy follows:]

PREPARED STATEMENT OF SENATOR PATRICK J. LEAHY

We will talk today about ISPs and URLs and other new language of the Internet age, but fundamentally we are continuing a 20-year-old conversation about how we assure the right of American people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures. This is both the promise and the mandate of our Constitution's Fourth Amendment.

The means by which law enforcement authorities may gain access to a person's private "effects" is no longer limited by physical proximity, as it was in the time of the Framers. New communications methods and surveillance devices have dramatically expended the opportunities for surreptitous law enforcement access to private messages and records from remote locations.

In short, new communications technologies pose both benefits and challenges to privacy and law enforcement. The Congress has worked successfully in the past to mediate this tension with a combination of stringent procedures for law enforcement access to our communications and legal protections to maintain their privacy and confidentiality, whether they occur in person or over the telephone, fax machine or computer. In 1968, the Congress passed comprehensive legislation authorizing government interception, under carefully defined circumstances, of voice communications over telephones or in person in Title III of the Omnibus Crime Control and Safe Streets Act.

We returned to this important area in 1986, when we passed the Electronic Communications Privacy Act (ECPA), which I was proud to sponsor, that outlined procedures for law enforcement access to electronic mail systems and remote data processing systems, and that provided important privacy safeguards for computer users. ECPA also set forth the procedures for use, application and issuance of orders for pen registers and trap and trace devices that were to be used to identify the numbers dialed from a particular telephone line or the originating number of an incoming telephone call, respectively. As the Committee's report on ECPA makes clear, these pen register and trap and trace orders were not to be used "to identify or record the contents of the communication." [Senate Comm. On the Judiciary, "Electronic Communications Privacy Act of 1986", S. Rep. No. 99–541, 99th Cong., 2d Sess. at p. 46 (1986).]

This hearing will explore where the FBI's use of the new surveillance tool called "Carnivore" fits into that mix.

As I understand this surveillance tool, Carnivore is a software program developed by the FBI and installed by the FBI at the physical premise of an Internet Service Provider to intercept Internet communications, in accordance with a court order. This court order may authorize capture of an entire communication, or it can be limited only to addressing information, akin to a pen register order for a telephone line. Carnivore is sufficiently versatile that the FBI can use the same program to accommodate variations in court order authorizations. I want to hear more about how the Carnivore program works, the precise kind of information the program produces to the FBI, and what controls the FBI has in place when Carnivore is used to insure the program is operated only as authorized by the applicable court order.

Certainly, some of the concern over the FBI's use of Carnivore stems from the fact that the Carnivore program is not "freeware" available for download and public scrutiny. I commend the Attorney General for her efforts to address this concern and for moving forward to hire an independent contractor to conduct a technical review of the surveillance program. This is constructive step to move beyond hypothetical discussions of Carnivore's theoretical capabilities to focus on the facts.

At the outset, let us be clear where there is no dispute. There is no dispute that the stringent legal requirements governing wiretaps apply to Carnivore when it is used to capture the content of e-mails or other computer transmissions. There is also no dispute that both the text and the subject line of an e-mail message are "content" which law enforcement may intercept only under a wiretap order. But fundamental questions remain about when the FBI chooses to use Carnivore, how the

program works, and whether the legal standards that apply to its use are adequate. First, telephone companies regularly comply with wiretap and other legitimate surveillance orders, as do Internet Service Providers. But if the trail of a criminal investigation leads to evidence in the custody of an Internet Service Provider that lacks the capability or willingness to conduct the interception as required in a court order, most of us agree that law enforcement authorities should not be stymied but should have the authority to pursue the trail. Indeed, it has been a long-standing tenet codified in the wiretap and pen register laws that providers of telephone services must furnish law enforcement officials with "all information, facilities and technical assistance necessary to accomplish" the interception or installation of the pen register device unobtrusively and with a minimum of interference with the service being provided to the person whose communications are to be intercepted." [18 U.S.C. §2518(4) and 3124(a).] Carnivore was apparently created for use in just this circumstantce—where the ISP is unable to assist directly in execution of the court-ordered surveillance.

We want to hear today about whether use of Carnivore is limited to only that circumstance and what effect, if any, this use has on the integrity and function of the ISP.

As the principal Senate sponsor of the Communications Assistance for Law Enforcement Act (CALEA), I should note that we passed this law in 1994 to require telephone companies to be able to execute court orders for surveillance. That law was passed with the concurrence of the telecommunications industry, which wanted all participants to share the responsibilities and expenses of complying with such court orders. This law exempts "information services", however, including most ISPs. Consequently, the FBI has developed its own program to fill the gap if a particular ISP is unable or unwilling to assist in execution of a court order for surveillance. This is preferable, in my view, to legislation requiring ISPs to ramp up to execute court orders.

*Second,* Carnivore apparently works by sifting through the Internet traffic of a particular ISP to capture the particular information or communication authorized by a court order. Privacy advocates are rightly concerned about whether Carnivore accesses too much—not only too much information about Internet users whose communications are not the subject of the court order, but also too much information about the communications that are the subject of the court order.

The Internet works by breaking communications down into separate packets that are reassembled at the destination point. The FBI says that, as a technical matter, Carnivore is able to find the different packets that make up a suspected criminal's Internet message only by sifting through all the traffic. This is cold comfort to all the other Internet users, who are not the subject of any court ordered surveillance but nonetheless are having their Internet messages automatically screened by the FBI's Carnivore program.

The FBI says that Carnivore can be used as the functional equivalent for the Internet of a pen register or trap and trace devices that provide information about the source or destination of a telephone call. Yet the addressing, or header, information on an Internet message may provide far more detail about the interests of the person sending the message than a dialed telephone number does. This prompts the question whether the same legal standard and procedure should apply to capturing Internet addressing information that applies to capturing telephone numbers.

*Finally,* Carnivore is a like a car. It can be useful, or it can be abused. What counts are the rules of the road and the license we give the driver. I am interested in hearing from the witnesses today whether the surveillance rulea we developed for the analogue telephone environment and for the pre-Internet computer environment are adequate to protect our current expectations of privacy when we go online.

I, for one, do not believe our current laws are adequate. That is why over a year ago I introduced the E-RIGHTS Act, S. 854, to update our laws and provide additional privacy protections for our online communications and records, including law enforcement access procedures and standards that are more in keeping with our current privacy expectations.

For example, a critical privacy issue confronting us today is the procedure by which law enforcement authorities obtain pen register and trap and trace orders. The controversy over Carnivore puts the shortcomings of that procedure in stark relief. Under current law, federal judges are no more than rubber stamps who are required to issue pen register or trap and trace orders whenever a prosecutor asks for them. Federal judges have no authority to ask "why" and to make aure that requested surveillance is necessary and justified. The E-RIGHTS Act proposes a procedure that would permit judges to ask for and get reasons for the surveillance. The Administration has recently transmitted proposed legislation that would modify this procedure in a fashion similar to the one I originally proposed.

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 searches. These principles can and must be respected when law enforcement agencies use surveillance tools to uncover and hold accountable criminal wrongdoers. I look forward to hearing from the witnesses today about whether Carnivore oversteps these bounds.

The CHAIRMAN. We have a distinguished group of witnesses here today. First, we will hear from Dr. Donald M. Kerr, who is the Assistant Director of the Federal Bureau of Investigation. Mr. Kerr heads the FBI lab that developed Carnivore and will be able to provide us with valuable insight from the Bureau.

Our next witness is Kevin V. Di Gregory, Deputy Assistant Attorney General of the Criminal Division, which includes the Computer Crimes and Intellectual Property Section at the Department of Justice.

After first hearing from these two witnesses, we will then hear from distinguished experts who will help guide us through the complex legal and technical issues involved in balancing the needs of law enforcement with the privacy rights of individuals.

So we will hear, after the first two, from Mr. Vinton G. Cerf of the Internet Society, a non-profit educational and research institution devoted to the continual evolution of the Internet. Mr. Cerf is also a senior vice president at WorldCom, where he is responsible for Internet architecture and technology. In 1997, Mr. Cerf was awarded the National Medal of Technology for his role in the invention and implementation of the Internet.

We are very fortunate to have you here today and we look forward to taking your testimony.

Our next witness, Michael O'Neill, is an assistant professor of law at the George Mason University School of Law in Fairfax, VA. Professor O'Neill, who is a former Supreme Court clerk and current Commissioner on the U.S. Sentencing Commission, specializes in criminal law, criminal procedure, and constitutional law.

Mr. O'Neill, we are very happy to have you back before the committee.

Next, we welcome James X. Dempsey, Senior Staff Counsel with the Center for Democracy and Technology, located here in Washington, DC. Mr. Dempsey is a respected leader in the privacy community. He has been a friend of the committee and has testified here before, so we are really happy to have you back and we look forward to hearing your testimony.

Our final witness is Professor Jeffrey Rosen, associate professor at the George Washington University Law School, located here in Washington. Professor Rosen teaches constitutional law, criminal procedure, and the law of privacy. He is also the legal affairs editor of the New Republic and has authored a book analyzing privacy issues.

I wouldn't mind having one of the books if you could send it, OK?

Mr. ROSEN. I will provide it for you Senator.

The CHAIRMAN. Good. I hope you autograph it.

Mr. ROSEN. Absolutely.

The CHAIRMAN. We are fortunate to have each of you here today and we want to welcome you to our hearing on "The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital

Age." This is a very, very important hearing and we look forward to hearing from each and every one of you.

So we will turn to you, Mr. Kerr, and go from there.

**PANEL CONSISTING OF DONALD M. KERR, ASSISTANT DIRECTOR, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC, ACCOMPANIED BY LARRY R. PARKINSON, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC; KEVIN V. DI GREGORY, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC, ACCOMPANIED BY MARTHA STANSELL-GAMM, CHIEF, COMPUTER CRIMES AND INTELLECTUAL PROPERTY SECTION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC; VINTON G. CERF, INTERNET TRUSTEE, INTERNET SOCIETY, RESTON, VA; MICHAEL O'NEILL, ASSISTANT PROFESSOR OF LAW, GEORGE MASON UNIVERSITY LAW SCHOOL, FAIRFAX, VA; JAMES X. DEMPSEY, SENIOR STAFF COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC; AND JEFFREY ROSEN, ASSOCIATE PROFESSOR OF LAW, GEORGE WASHINGTON UNIVERSITY LAW SCHOOL, WASHINGTON, DC**

**STATEMENT OF DONALD M. KERR**

Mr. KERR. Good morning, Mr. Chairman, members of the committee. I am grateful for the opportunity to discuss the Internet and data interception capabilities developed by the FBI in response to the increased exploitation of computers, networks, and databases by terrorists, spies, and dangerous criminals to commit crimes and to harm the safety, security and privacy of others.

I have provided a rather long statement for the record which I will spare you.

The CHAIRMAN. We will put all statements in the record as though they were fully delivered. We hope you can summarize.

Mr. KERR. Thank you, Mr. Chairman, and I will simply briefly try to address some of the major issues covered in that statement.

The context for our development and use of the Carnivore e-mail intercept system and other similar tools is the significant increase in terrorist and criminal acts. For example, terrorist groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate relatively securely.

An early instance of the use of secured information was the convicted terrorist Ramzi Yousef, who was the mastermind of the World Trade Center bombing, who, in fact, had encrypted files on his laptop for blowing up U.S. airplanes in various parts of the world.

Serious fraud, such as the one mentioned earlier in your opening statement, recently dramatized by a case in New York, in March, where 19 people were charged in an insider trading scheme—the commission of that fraud rested on the ability to enter chat rooms, in effect recruit people to provide information on two major brokerage firms' customers and, of course, share in the profits from the use of that illicitly obtained information.

You are well aware of our Innocent Images program dealing with child pornography and sexual exploitation of children where, since

1995, the FBI has investigated nearly 800 cases involving adults traveling interstate to meet minors for the purpose of illegal sexual relationships, and more than 1,800 cases involving persons trading child pornography over the Internet.

As mentioned, the FBI only conducts electronic surveillance pursuant to Federal law, and in particular acts pursuant to court order. The Federal electronics surveillance law has carefully balanced the constitutional and privacy rights of individuals, legitimate search and seizure needs of law enforcement, and the obligations placed upon communications and information service providers to cooperate.

In enacting the Federal electronic surveillance laws, including title III and the ECPA-based transactional record and pen register trap and trace regimes, Congress specified appropriately strict procedures for law enforcement's interception of communications content, and also its access to communications transactional, addressing, and dialing information.

Also, by law, the investigators must specify the steps that will be taken to minimize the acquisition of any non-criminal communications. A title III application must be approved by a Federal district court judge who, after authorizing the order, carefully monitors the progress of the surveillance by reviewing reports brought to the court usually every 7 to 10 days by the U.S. Attorney's Office. The U.S. Attorney's Office oversees the surveillance on a daily basis, and at the end of the surveillance the judge directs notice be given to those whose communications were intercepted.

Under titles II and III of ECPA, law enforcement acquires transactional addressing and dialing type information pursuant to court orders based upon relevancy to an ongoing criminal investigation. These acquisitions, which include no communications content, can be obtained through approval by a Federal magistrate pursuant to applications from the U.S. Attorney's Office.

Acquisitions under the pen register trap and trace regime last for 60 days, since they only pertain to the transactional addressing and dialing information. While the law requires no notice be given to the criminals or others concerning whom service provider communications transactional records are obtained, many service providers advise their subscribers after the investigation is concluded.

Those who have raised concerns regarding Carnivore have principally asserted that through the use of Carnivore, the FBI is collecting more information than a given pen register or trap and trace court order permits. I want to speak to the safeguards we have in place, the techniques by which we deploy Carnivore, and in particular I think the great protections we offer for both personal privacy and the business interests of the Interest service providers.

First of all, as you have correctly mentioned, Carnivore is both software and hardware. And because it is software in part, it can be configured to specifically comply with each court order. In doing that, we provide an audit trail. And, of course, you are well aware of the sanctions for misuse, both criminal and civil.

It is a PC-based system. We maximize the use of commercial software to reduce risk and cost. It is installed by a team comprising a senior supervisory FBI special agent, typically an elec-

tronics technician, and one or more members of the Internet service provider's staff to be sure that we don't do something that would interfere with their system. But I would point out the case agent is not the one installing the system. People who are specifically trained in its use and the legal constraints on its use are the ones who do that.

It is important to understand that it filters the Internet traffic. It is looking for the addressing information, and at the first stage it is looking for the Internet addresses that are covered in the court order and it picks off the packets that meet that test. It then goes through the subsequent filtering stage. If full content is allowed, it, of course, captures all of the packets relating to that message and records them in their digital form. If only the addressing information, the "to" and "from" lines, subject again to the court order, are captured, those are recorded.

Once the recordings are made, there is no other information available to the FBI. We capture and record no other information, and those pieces of data are not available to us at any subsequent time. There is no real-time review of text because, in fact, we are dealing with systems where the information is transiting at rates, for instance, of 40 megabits a second. We have no one who can read 0s and 1s at 40 megabits a second and translate that into content. In fact, we only restore the message when content is authorized after recovering the recorded bits and bringing it back to our laboratory to recover the actual content of the message.

We produce a record of all settings, and that becomes part of the evidentiary chain that we create. The system, in fact, is secured within the Internet service provider's spaces to provide physical chain of custody as well. In fact, in the newest version that we are intending to bring into use, we will provide the same authentication of the message information that we capture, as well as the settings, so that we will be able to testify later in court as to what the settings were, who set them up, and were any subsequent changes or alterations made.

Carnivore does not adversely affect the business interests of the Internet service provider. I mentioned we safeguard their interests in part by collaborating with their technical staff. We always use the smallest segment of traffic through their system because, in fact, what we are after is just the message traffic of the subject of the court order. So if that can be delivered and the ISP can do it with their equipment, we accept that from them and, in fact, we reimburse them for providing that service.

When the ISP does not have the equipment or the capability to meet the terms of the court order, we, in fact, use Carnivore, installed under the conditions that I mentioned. But recall there may be 15,000 ISP's in this country. Some of them are well capitalized and well equipped. Others are very small operations and would not have the capital to have in place an infrequently used capability or perhaps a never used capability.

The CHAIRMAN. How many ISP's did you say are in the country?

Mr. KERR. I think approximately 15,000, but I think there are others at the table who know better.

Mr. CERF. Mr. Chairman, I can respond to that. I think probably that is a global number, as opposed to the number in the United

States. So presumably your focus of attention is the number in the United States, but that still could be on the order of 8,000. So you are in the same order of magnitude.

The CHAIRMAN. OK; sorry to interrupt you.

Mr. KERR. Not a problem. It is very helpful.

Carnivore is a passive system and, in fact, it is isolated from the Internet service provider's network by a commercial device that allows for information to flow to Carnivore, but for no signals to flow from Carnivore into the system. And, of course, like all communications intercept equipment, it is removed as soon as the court order has expired.

Overall, we think that the public should have trust and confidence in the FBI conduct of electronic surveillance under the legal guidance that we have. We first exhaust other means to get timely information. We always try to minimize the intrusiveness of our intercept, whether it be for e-mail or for telephones.

We attempt to avoid undesirable consequences for telecommunications providers or Internet service providers. We cannot activate our capabilities without an appropriate order. There are sanctions in place that deter misuse. Broad search and surveillance is prohibited, and we seek specific evidence of criminal behavior, not broad information content.

With that, Mr. Chairman, I will conclude my remarks and look forward to your questions.

[The prepared statement of Mr. Kerr follows:]

PREPARED STATEMENT OF DONALD M. KERR

Good morning, Mr. Chairman and Members of the Committee. I am grateful for this opportunity to discuss with you the FBI's Carnivore system—a system specially designed for effectively enforcing the law while at the same time fully complying with the law. Carnivore is a system which we are counting on to help us in critical ways in combating acts of terrorism, espionage, information warfare, hacking, and other serious and violent crimes occurring over the Internet, acts which threaten the security of our Nation and the safety of our people. In my statement, I will touch upon five points; why we need a system like Carnivore; why the public should have confidence that the FBI is lawfully Carnivore; how Carnivore, as a special purpose electronic surveillance tool, works; why computer network service providers, with whom the FBI always work closely, should not be fearful about Carnivore's use with their networks; and, as an overarching matter, why the public should have trust in the FBI's conduct of electronic surveillance and in its use of the Carnivore system. In addressing these important points, we hope to set the record straight and allay any legal, privacy, network security, and trustworthiness concerns.

*Why does the FBI need a system like Carnivore?*

By now, it has become common knowledge that terrorists, spies, hackers, and dangerous criminals are increasingly using computers and computer networks, including the Internet, to carry our their heinous acts. In response to their serious threats to our Nation, to the safety of the American people, to the security of our communications infrastructure, and to the important commercial and private potentialities of a safe, secure, and vibrant Internet, the FBI has responded by concentrating its effort, including its technological efforts, and resources, to fight a broad array of Cyber-crimes.

While the FBI has always, as a first instinct, sought to work cooperatively and closely with computer network service providers, software and equipment manufactures, and many others to fight these crimes, it also become obvious that the FBI needed its own tools to fight this battle, especially where legal, evidentiary, and investigative imperatives required special purpose tools. One such tool is Carnivore, which I will discuss at length today. However, before discussing Carnivore, it is important to identify and briefly discuss some of the types of Cyber-crime threats which we in law enforcement have been encountering, and will encounter in the fu-

ture, and concerning which Carnivore, and tools such as Carnivore, are of critical importance to the FBI.

*Terrorism*

Terrorist groups are increasingly using new information technology (IT) and the Internet to formulate plans, raise funds, spread propaganda, and communicate securely. In his statement on the worldwide threat in the year 2000, Director of Central Intelligence George Tenet testified that terrorist groups, "including Hezbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, E-mail, and encryption to support their operations." As one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer.

Other terrorist groups, such as the Internet Black Tigers (who are reportedly affiliated with the Tamil Tigers), engaged in attacks on foreign government websites and E-mail servers. "Cyber terrorism"—the use of Cyber tools to shut down critical national infrastructures (such as energy, telecommunications, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population—is emerging as a very real threat.

Recently, the FBI uncovered a plot to break into National Guard armories and to steal the armaments and explosives necessary to simultaneously destroy multiple power transmission facilities in the Southern United States. After introducing a cooperating witness into the inner circle of this domestic terrorist group, it became clear that many of the communications of the group were occurring via E-mail. As the investigation closed, computer evidence disclosed that the group was downloading information about Ricin, the third most deadly toxin in the world. Without the fortunate ability to place a person in this group, the need and technological capability to intercept their E-mail communications' content and addressing information would have been imperative, if the FBI were to be able to detect and prevent these acts and successfully prosecute.

*Espionage*

Not surprisingly, foreign intelligence services have adapted to using Cyber tools as part of their espionage trade craft. Even as far back as 1986, before the worldwide surge in Internet use, the KGB employed German hackers to access Department of Defense systems in the well-known "Cuckoo's Egg" case. It should not surprise anyone to hear that foreign intelligence services increasingly view the Internet and computer intrusions as useful tools for acquiring sensitive U.S. government and private sector information.

*Information Warfare*

The prospect of "information warfare" by foreign militaries against our Nation's critical infrastructures is perhaps the greatest potential Cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional weapons, nations see Cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel—our growing dependence on information technology in government and commercial operations. Two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States. And a Russian official has also commented that an attack on a national infrastructure could, "by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction."

*Child Pornography and Sexual Exploitation of Children*

Through the FBI's "Innocent Images" case, and others, it has become abundantly clear that certain adults are using computers and the Internet widely to disseminate child pornography and to entice young children into illegal and often violent sexual activity. Such sexual predators find the Internet to be a well-suited medium to trap unwary children. Since 1995, the FBI has investigated nearly 800 cases involving adults traveling interstate to meet minors for the purpose of illegal sexual relationships, and more than 1850 cases involving persons trading child pornography—almost all of these involve the exchange of child pornography over the Internet.

*Serious Fraud*

One of the most serious criminal threats facing the Nation is the use of the Internet for fraudulent purposes. For example, securities offered over the Internet have added an entirely new dimension to securities fraud investigations. The North

American Securities Administrators Association has estimated that Internet-related stock fraud results in a loss to investors of approximately $10 billion per year (or nearly $1 million per hour). In one case, on March 5, 2000, nineteen people were charged in a multimillion-dollar insider trading scheme. At the core of the scheme, the central "insider" figure went online and found others in ISP chat rooms. He soon was passing inside information on clients of several brokerage firms to two other individuals in exchange for a percentage of any profits they earned by acting on it. For 2½ years, this person passed inside information, communicating almost solely through online chats and instant messages, with the insider receiving $170,000 in kickbacks while his partners made $500,000.

*Why should the public have confidence in the FBI's lawful use of Carnivore?*

There are a number of reasons why the public should have confidence in the FBI's lawful use of Carnivore. First of all, since 1986, with the enactment of the Electronic Communications Privacy Act of 1986 (ECPA), which amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), Congress created statutory legal protection for all types of wire and electronic communications' content, including computer and Internet-based communications' content, consistent with the Constitution. The ECPA also created statutory privacy protection for "transactional records" pertaining to an electronic communications provider's provision of services to a customer or subscriber consistent with the Constitution. The term "transactional records," as used here, includes addressing (e.g., in the context of E-mail communications, the "to" and "from" lines—but not the "subject" or "re" lines) routing, billing, or other information maintained or generated by the service provider. "Transactional records" do not include the content (substance, purport or meaning) of E-mails or other communications. Correspondingly, in the ECPA, Congress regulated all governmental electronic surveillance interceptions of communications' content and all acquisitions of communications addressing and transactional record information consistent with the Constitution. Under the ECPA, all such electronic surveillance efforts require some form of court order, either a full Title III (probable cause-based) court order for obtaining communications' content or an ECPA-created court order based upon relevancy for communications' addressing and transactional record information. Of course, there are "emergency" provisions whereby surveillance is permitted to proceed immediately, when high-level Department of Justice authorization is obtained, so long as a court order is filed within 48 hours.

Under Title III, applications for electronic surveillance must demonstrate probable cause and state with particularly and specificity: the offenses being committed, the communications facility regarding which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted. Clearly, the criminal electronic surveillance laws focus on gathering hard evidence—not intelligence. Under this law, the FBI cannot, and does not, "snoop."

In obedience of the law, the FBI obtains judicial authorization, in terms of always obtaining the appropriate court order required when intercepting wire and electronic communications' content or when acquiring addressing information and transactional record information, or lawful consent, regardless of whether they are occurring over a computer or telecommunications network. The FBI's use of the Carnivore system—approximately 25 times in the last two years—has in every case and at all times been pursuant to such a judicially-granted court order or lawful consent. In every case, we only deploy Carnivore after serving a court order on an ISP (or after obtaining lawful consent of a party to the communication) and then only after working closely with the ISP technicians or engineers in installing it. Parenthetically, were the ISP is equipped to fully and properly implement the court order or consensual authorization, the FBI leaves the interception to the ISP and does not rely upon Carnivore. Moreover, if an FBI employee were to attempt to acquire such content or information using Carnivore without obtaining a court order or appropriate consent, it would be a serious violation of the law—a federal felony, thereby subjecting the employee to criminal prosecution, civil liability, and termination. Finally, FBI employees fully understand that the unlawful interception of the content of private communications will lead to the suppression of any and all tainted evidence and any evidence of fruits derived therefrom. In short, the penalties for violating the electronic surveillance laws are so severe as to dissuade any such unlawful behavior, even if someone were so inclined.

Those who have raised legal concerns regarding Carnivore have principally asserted that (1) through its use of Carnivore, the FBI is collecting more information than a given pen register or trap and trace court order permits, or (2) while using Carnivore, the FBI is acquiring more information under such order than that order should lawfully permit.

As to the first assertion (as will be explained in detail below), in many investigative situations (principally those involving pen register or trap and tract court orders), Carnivore—far better than any commercially-available sniffer—is configurable so as to filter with precision certain electronic computer traffic (i.e., the binary computer code, the fast-flowing streams of O's and 1's) such that, in each case, FBI personnel only receive and see the specified communications addressing information associated with a particular criminal subject's service, concerning which a particular ECPA court order has been authorized. Further, to our knowledge, there are few, if any, electronic surveillance tools that perform like Carnivore, in terms of its being able to be tailored to comply with different court orders, owing to its ability to filter with precision computer code traffic.

In fact, the genesis for some of the technological functionality of Carnivore was the result of the FBI's decision, made in light of privacy and investigative concerns, that prudent practice, with regard to computer network-based electronic surveillance, dictated that the communications' addressing information gleaned through technical equipment the FBI would be using should, to the fullest extent possible, correspond to that information authorized for acquisition and use under law. In this regard, prior to our development of Carnivore, the FBI, consistent with the Constitution and the legal mandate found in 18 U.S.C. 3121, was using "technology reasonably available to it" which permitted the acquisition of communications' addressing information, but which necessitated minimization. However, while the technology then available (principally commercial sniffers) worked as well as could be expected, as discussed in greater detail below, such equipment had never been designed as a law enforcement electronic surveillance tool, and hence had shortcomings. Not knowing if, or when, market forces would lead to the development of a law enforcement electronic surveillance too, the FBI took the initiative.

In this context, we want to make sure that both the Congress and the public understand that, in using Carnivore, there is no broad-brush acquisition by either Carnivore or by FBI personnel of the "contents of the wire or electronic communications" of all ISP users—such as to constitute an unauthorized Title III "intercept." Carnivore only intercepts the communications of that particular criminal subject for which a Title III order has been obtained. Similarly, we want everyone to understand that, in using Carnivore, there is no broad brush collection, storage, or review, by either Carnivore or by FBI personnel, of the addressing or transactional information regarding any ISP user beyond that pertaining to the criminal subject's service for which an ECPA court order under 18 U.S.C. 3123 and 18 U.S.C. 2703(c)(d) has been obtained.

As to the second assertion, some have stated that, in their opinion, the FBI is acquiring more information when it uses Carnivore to acquire communications addressing and transactional record information than it should be entitled to under the Constitution or under the ECPA statutory regimes found in Chapters 206 and 121 of Title 18 of the United States Code, and, in particular, under the court order authorities within 18 U.S.C. 3123 and 18 U.S.C. 2703(c)(d). By way of response, and more to the point, it appears that much, if not most, of this contention regarding governmental access to communications addressing and transactional information emanates from concerns about the use of electronic surveillance generally, as opposed to the FBI's use of Carnivore in particular. However, there is little or nothing in law or Federal jurisprudence to support the contention that has been asserted in this regard.

In 1979, the U.S. Supreme Court ruled that, because there was no justifiable or reasonable expectation of privacy in the electronic impulses dialed and transmitted over the telephone lines of a service provider to initiate a telephone call, no Fourth Amendment search or seizure was implicated, and, accordingly, that no legal right or protection regarding governmental acquisition of such information was cognizable or afforded under the Constitution (see, *Smith* v. *Maryland*, 442 U.S. 735 (1979). Similarly, the U.S. Supreme Court had earlier found no Constitutional right or protection against the Government's warrantless acquisition of banking information that had been disclosed by a customer to a third party financial institution (see, *United States* v. *Miller*, 425 U.S. 435, 442–444 (1976)). Hence, then, at least as a matter of Constitutional law, the Supreme Court has found no Constitutional requirement for a probable cause-based warrant in order to acquire transactional records or information that a customer conveys or transmits to third parties such as banks and telephone service providers.

In 1986, in enacting the ECPA's Title II and Title III provisions, the Congress was aware of the foregoing Supreme Court rulings and sought to "create" new privacy protection in statute to protect a subscriber's communications addressing and transactional record information. Also, just as it intended to afford statutory privacy protection for such information, Congress also created appropriate and commensurate

court order authorities for lawful governmental use in acquiring such information. In doing so, Congress made very reasonable, considered, and balanced determinations as to the level of privacy protection that was appropriate for each type of information at issue. Now, although it is true that there have been great changes in computer technology since 1986, the core statutory privacy principles and fault lines applicable to protecting computer-based communications content, on the one hand, and communications addressing information, on the other, as well as to their lawful interception or acquisition, have remained quite stable.

Since 1986, and long before the advent and use of Carnivore, the FBI and many other Federal, State, and local governmental authorities having been lawfully acquiring computer network-based addressing and transactional information from both telecommunications carriers and Internet Service Providers (ISPs) under court order as anticipated by Congress within the ECPA., i.e., the court order authorities set forth within 18 U.S.C. 3123 and 18 U.S.C. 2703(c)(d). Governmental surveillance in this area has proceeded based upon the rightful premise that, with the appropriate ECPA court order(s), each and every type of communications addressing and transactional record information found within telecommunications and computer networks could be lawfully acquired. Since the ECPA was enacted, federal courts throughout the country have consistently authorized ECPA-based court orders applied for by the Department of Justice and the United States Attorneys' Offices, under the authorities set forth within 18 U.S.C. 3123 and 18 U.S.C. 2703(c)(d), with regard to the types of governmental access to and acquisition of computer network addressing information currently being complained of, without finding Constitutional or statutory impediment.

Finally, with specific reference to Carnivore, in the approximately 25 instances wherein its use has occurred, the courts have approved the applications, in terms of what was lawfully obtainable through the federal statutory regimes(s) and/or court orders cited above, and in terms of the information which Carnivore, through its filtering, enables FBI personnel to lawfully receive or see under these regimes. In the only case challenging Carnivore's intended use (in a case involving the acquisition of E-mail addressing information under the court order authorities set forth within 18 U.S.C. 2703(c)(d) and 18 U.S.C. 3123), the court sided with the Government, finding that the addressing information to be acquired through the Government's use of Carnivore was no more intrusive than the information acquired through a conventional pen register under 18 U.S.C. 3123.

*How does Carnivore work, and why the FBI believes Carnivore is superior from a legal, privacy, investigative, evidentiary and technological perspective to commercial sniffers*

Carnivore is very effective and discriminating special purpose electronic surveillance system. Carnivore is a filtering tool which the FBI has developed to carefully, precisely, and lawfully conduct electronic surveillance of electronic communications occurring over computer networks. In particular, it enables the FBI, in compliance with the Constitution and the Federal electronic surveillance laws, to properly conduct both full communications' content interceptions and pen register and trap and trace investigations to acquire addressing information.

For many electronic surveillance purposes, Carnivore is superior to any commercially available "sniffer" tool which ISP network administrators typically might use for network oversight, management, and trouble-shooting. In the ISP world such sniffers are the closest thing to what would be considered an electronic surveillance interception device. Such sniffers, however, were never designed or intended to be a special purpose electronic surveillance tool, and therefore they are not best suited to protect the privacy rights afforded by the Constitution or by statute.

It's important to describe the context of when and how Carnivore is used and the way Carnivore works. It's most critical to clearly understand what Carnivore discloses and, more importantly, what it does not disclose to the FBI personnel who use it.

First of all, as emphasized above, Carnivore is only employed when the FBI has a court order (or lawful consent) authorizing a particular type of interception or acquisition regarding a particular criminal subject user, user address, or account number. Second, when an ISP can completely, properly, and securely comply with the court order on its own, the FBI does not need to deploy Carnivore.[1] Third, if a deci-

[1] In many instances, ISPs, particularly the larger ones, maintain certain technical capabilities which allow them to comply, or partially comply, with court orders. For example, certain ISPs have the capability to intercept or "clone" the E-mail transmitted to and from a particular criminal subject's account. In many instances, such capabilities are satisfactory and allow full compliance with a court order. However, as noted in the main text, in most cases, ISPs do not have

sion is made to use Carnivore, the FBI never deploys it without the cooperation and technical assistance of the ISP technicians and/or engineers. Fourth, through working with the ISP, Carnivore is positioned and isolated in the network so as to focus exclusively upon just that small segment of the network traffic where the subject's communications can be funneled. This is roughly analogous to using an electronic surveillance device only within in a single trunk or cable within a telephone network. Stated differently, and contrary to the statements of some critics, Carnivore is not positioned to filter or access "in a Big Brother mode, all subscriber traffic throughout an ISP network."

In illustrating its functionality, it is important to understand that Carnivore's filtering operates in stages. Carnivore's first action is to filter a portion of an ISP's high speed network traffic. Specifically, it filters binary code—streams of 0's and 1's that flow through an ISP network, for example, at 40 mega-bits per second, and often at much higher speeds. Carnivore operates real time with these speeds. To visualize this, imagine a huge screen containing 40 million 0's and 1's flashing by on this screen for one second, and for one second only. Carnivore's first effort—entirely within the Carnivore box—is to identify within those 40 million 0's and 1's whether the particular identifying information of the criminal subject (for which a court order has been authorized) is there.

If the subject's identifying information is detected, the packets of the subject's communication associated with the identifying information that was detected, and those alone, are segregated for additional filtering or storage. However, it's critically important to understand that all of those 40 million 0's and 1's associated with other communications are instantaneously vaporized after that one second. They are totally destroyed; they are not collected, saved, or stored. Hence, FBI personnel never see any of these 40 million 0's and 1's, not even for that one second. Continuing the illustration, if the subject's identifying information is not in that screen, then the next screen of 40 million 0's and 1's flashes by at the same rate, and the process described above is repeated in identical fashion until the subject's identifying information is detected.[2]

After exclusively segregating the subject's information for further machine processing, then a second stage of filtering is employed. At this point, and again all within the Carnivore box, Carnivore checks its programming to see what it should filter and collect for processing. In other words, it determines, as required by the specific wording of the court order, if it's supposed to comprehensively collect communications content—in a full title III or FISA mode—or, alternatively, whether it's only to collect pen register or trap and trace transactional and addressing information. Only information specified in the court order is being collected by Carnivore.

Importantly, this is where some of Carnivore's key legal, evidentiary, and privacy-enhancing features really kick in. To address the particular concerns that have been raised regarding what is filtered and processed, and what FBI personnel see and don't see, its useful to illustrate how Carnivore operates, for example, in a pen register or trap and trace transactional and addressing information mode, pursuant to authorities set forth within 18 U.S.C. 3123 and 18 U.S.C. 2703(c)(d). Under these circumstances, Carnivore only collects transactional and addressing information. It is programmed to filter out all content, including subject line and "re" information.

---

such capabilities or cannot employ them in a secure manner. Also, most "off the shelf" sniffers or internal systems designed ad hoc to effect an electronic surveillance effort frequently lack the ability to properly discriminate between messages in a fashion that satisfies the court order. Further, many court orders go beyond E-mail, authorizing the acquisition of other messages or protocols, such as instant messaging. In these cases, obviously, a cloned mailbox would not be sufficient to comply with the order of the court.

[2] Parenthetically, some might argue that although the FBI does not collect, save, or store all of those 40 million bits per second, that it could if it chose to. In fact, that is simply not the case. The reason is that, even with substantial gigabit level storage, the hard drive storage would fill up in a matters of a few minutes, requiring constant replacement of the hard drives or alternatively the front end acquisition of large amounts of equipment space within an ISP's access space. Neither one of these scenarios is in any way realistic.

But, for the sake of argument, even if such massive collection and storage could be marshaled, an equally gigantic effort would be required to process all of the O's and 1's to produce intelligible English text. Then finally, there would have to be a huge dedication of FBI human resources to sift through the information—and for no discernable reason. The fact of the matter is that the FBI, focused upon the identified criminals/accounts under investigation, is normally "swamped" with evidence. The FBI simply has no interest in rummaging ("snooping") through the immense number of communications of those ISP users that through mere happenstance traverse the same part of the network as the traffic of the criminal subject. As noted above, any such unauthorized rummaging would be a violation of law, subjecting FBI personnel to criminal prosecution, civil liability, and immediate termination of employment.

For example, certain pen register or trap and trace orders will authorize collection of simply "source," "destination," date, time, and duration of the message. Others will authorize collection of "source," "destination," "user account address," date, time, and duration. Again, each collection, and the filters being employed, are tailored to a particular court order's authorization.

At this point, an explanation on a more technological and functional level is warranted as to why, with regard to pen register and trap and trace transactional and addressing information usage, Carnivore's use was necessitated by certain privacy, evidentiary, and investigative concerns. Commercially-available sniffers do a very good job in many circumstances of filtering and segregating ISP information, especially in title III interceptions. However, in other cases, where more stringent legal, evidentiary, and law enforcement investigative requirements exist, many sniffers would collect either too much information, such as collecting *all* of the information regarding a given criminal subject's account, or , alternatively fail to collect the authorized information at all.

For example, because of differences and vagaries in network protocols and header addressing information and their implementations by ISPs, collections with these commercial sniffers often do not cut off the header addressing information at the precise point. This can lead to a small amount of a communications' content being included (such as the "subject line") which then must be minimized by human review. Hence, resort to commercial sniffers alone under certain circumstances raises privacy concerns and interferes with the FBI's investigative resources. While such sniffer capabilities might suffice for non-law enforcement administration purposes, it is less than perfect for a law enforcement point of view. Carnivore's development was driven by a need to address such issues.

In another area with significant legal, evidentiary, and investigative ramifications, Carnivore is superior to commercial sniffer. Commercial sniffers are typically designed to work only with fixed IP addresses. Unfortunately, dynamic addressing within ISPs occurs probably in 98–99% of the cases. Hence, the use of commercial sniffers, without more, would be ineffective in 98–99% of court authorized collections. Carnivore was specifically designed to interface with ISP networks so that when dynamic addressing occurs it can immediately respond to it. Finally, while it is true that other efforts with ISPs can address this problem, this problem is effectively and efficiently resolved technically by Carnivore.

In still another area with significant legal, evidentiary, and investigative ramifications, Carnivore has the ability to filter and collect Simple Mail Transport Protocol (SMTP) traffic sent to or from a specific user. Most, if not all, commercial sniffers would collect all E-mails and then require a human visual search to find the targeted E-mail. This obviously is wanting from a privacy and operational perspective. Carnivore, on the other hand, has the ability to conduct very surgical acquisitions of only a targeted criminal subject's E-mail.

To repeat, during all the filtering/processing noted above, no FBI personnel are seeing information—all of the information filtering/processing, and purely in a machine-readable format, is occurring exclusively "within the box."

Now, at the end of all the filtering and processing, there, of course, is information that ultimately is collected and stored for human review. Hence, what finally reaches the hands of FBI personnel in every case is simply and only that particular lawfully authorized by the court order—and no more.

Finally, Carnivore includes another piece of important functionality. For evidentiary purposes, and as an audit history, Carnivore was also designed to append to an event file for each collection the filter configuration that was used in that collection. This information tells the FBI personnel—and indeed it tells the world, including a court, defense counsel, and a jury—what mode the device was operating in (what it was programmed to collect), so as to allay any suspicion that more information was being passed along to FBI personnel.

As you know, Rule 901 of the Federal Rules of Evidence requires the authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications establishes, with much less human interaction and without the potential for human error, a trustworthy machine-based memorialization of the evidence. It also establishes a reliable first link in an undisturbed chain of custody, and it facilitates the ease and accuracy of a witness' testimony by permitting the witness to testify as to the retrieval of the evidence and as to the purely technological method by which the evidence was acquired and recorded. Finally, Carnivore is being upgraded by adding an integrity feature which will further demonstrate the authenticity of the information, by imprinting on the evidence the collection mode being used. It thus helps prove authenticity, by demonstrating that no alteration has been made to the filter settings employed or

to the information obtained. As an evidentiary matter, such features strengthen showings of "chain of custody," authenticity, and non-alteration.

*Why computer network service providers should not be fearful about Carnivore's use with their networks*

Notwithstanding assertions to the contrary, the Carnivore system is safe to operate with IP networks. As noted above, Carnivore is only installed in that small segment of the computer network through which the criminal subject's communications traffic will pass. The Carnivore system is connected with the network by a bridging device that physically prevents Carnivore from transmitting into the network. Thus, as a technological certainty, there is absolutely no way it could possibly have any ability to transmit any information or thing into the network.

Importantly, Carnivore is only attached to the network after consultation with, and after obtaining the agreement and assistance of, technical personnel form the ISP. It is worth noting that, to date, the FBI has never installed Carnivore with an ISP's network without first obtaining the assistance of the ISP's technical personnel. The Internet is highly complex and heterogeneous environment in which to conduct electronic surveillance, and I can assure you that without the technical knowledge of the ISP's personnel, it would be very difficult, and in some instances impossible for law enforcement agencies to act unilaterally and successfully in implementing such a technical effort. Moreover, the FBI particularly depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Some critics have also asserted that the use of the Carnivore system introduces significant new vulnerabilities for hacking access. But such assertions miss the mark. With regard to hacking, and considering the hacking methodologies most commonly employed, there would be absolutely no greater qualitative value in trying to use the Carnivore system as an access point than any other access point or node in the Internet, concerning which there are literally millions. Indeed, recognizing that Carnivore is a law enforcement surveillance tool, a hacker's attempted use of it as an access path would be particularly foolish inasmuch as access to Carnivore, as noted above, would never create an actual transmission path into the network.

Lastly, there has been the suggestion, in prior Congressional testimony, that the Carnivore system had caused a network crash or other problems in the network of a particular ISP. Let me emphasize that such a suggestion is simply factually incorrect. In the instance cited, the cause of the network problem (there was no crash)—it was in the nature of a network slowdown—was programming steps undertaken exclusively by the ISP's technicians, and entirely on their own.

*Why should the public have trust in the FBI's conduct of electronic surveillance, and, in particular, in its use of the Carnivore system*

We believe that the American public should have trust in the FBI's conduct of electronic surveillance, principally because it has an outstanding record of lawfully complying with the Federal electronic surveillance laws which the Congress first enacted over thirty years ago, in 1968. Although the assertion of widespread 'illegal FBI wiretapping' is frequently made, and is an article of faith for some, the facts in no way support it. Any careful review of the dockets of the Federal courts offers no support to the assertion of FBI electronic surveillance abuse during these years. Indeed, all FBI electronic surveillance is authorized and carefully supervised by many different "outside" entities.

To begin with, in every FBI investigation involving electronic surveillance, all surveillance efforts are approved, monitored, and overseen at each step of the way by both the local United States Attorneys Office and the appropriate U.S. District Court Judge (for Title IIIs) or Magistrate (for ECPA court orders). In surveillance conducted under the Foreign Intelligence Surveillance Act (FISA), FBI surveillance efforts are approved, monitored, and overseen by the Department of Justice's Office of Intelligence Policy and Review, and by the Foreign Intelligence Surveillance Court, respectively. Moreover, before any full-blown Title III or FISA electronic surveillance involving the interception of communications' content is approved, lengthy, multi-layered, and thorough reviews occur both within the FBI and within the Department of Justice, and, as a statutory mandate, high-level Department of Justice approval is required for all such surveillance.

For more than three decades now, FBI electronic surveillance has been closely supervised and monitored by the Department of Justice. There has been no indication of FBI abuse. Indeed, the Department of Justice typically points to the FBI as an agency model with regard to how to carefully and lawfully conduct electronic surveillance.

Aside from Executive and Judicial Branch review of FBI electronic surveillance efforts, the Congress itself exercises frequent and ongoing oversight over the FBI's conduct of electronic surveillance in a number of ways. Year in and year out, numerous Congressional Committees (and their staff) involved in authorizations and appropriations scrutinize FBI expenditures, programs, and even equipment. Committees on the Judiciary and Intelligence frequently hold hearings, such as this, and submit written questions to be addressed by the FBI. Further, since Title III's enactment in 1968, the Congress has revisited the Federal electronic surveillance laws on a number of occasions: in 1978 (FISA), in 1986 (ECPA), and in 1994 (CALEA). And, as the Committee is well aware, each time the Federal electronic surveillance laws are updated there is a substantial subtext to the legislative initiative wherein the Congress considers and reconsiders whether such laws are working well and whether there is any significant indication of abuse such as to warrant the laws' curtailment or modification. However, with each of these pieces of legislation, the Congress has never found or suggested that the law enforcement community, in general, or the FBI, as an agency, in particular, was abusing the electronic surveillance authorities.

Further, in recent years, it has become somewhat commonplace for members of the Congress to request a visit to the FBI's Engineering Research Facility (ERF) to permit themselves and/or their staff to understand FBI surveillance methodologies, etc., better. Beyond these, every year the Administrative Office of the United States Courts sends to the Congress the yearly "Wiretap Report" which specifies Federal, State, and local law enforcement's Title III electronic surveillance activities. Likewise, and also pursuant to Federal statute, every year the Department of Justice submits to the Congress a report regarding the use of pen register and traps and traces conducted by law enforcement agency components within the Department. Further, several years ago, as a part of the Anti-terrorism and Effective Death Penalty Act of 1996, the Congress requested a Report from the Department of Justice which was to specifically include a review of any abuse in law enforcement's conduct of electronic surveillance. In the Report submitted by the Department of Justice, it was pointed out that law enforcement errancy in this area was rare, and did not suggest any significant problem. In particular, there was no citation as to abuse by the FBI.

At this point, it may be useful to briefly discuss another vital component in the overall electronic surveillance/Carnivore mix: the FBI personnel who use it.

In this regard, the Committee would truly be missing a significant part of the story if we failed to point out the quality of the FBI personnel involved and the ways in which they perform their tasks. To begin with, to become and FBI employee requires a substantial showing of trustworthiness, lawfulness, and personal and professional intergrity—all of which must be demonstrated through the conduct of an extensive and very thorough national security-level background investigation. To be sure, the structure of the FBI would quickly collapse if the agency and all of its onboard employees could not trust without reservation its new employees. And the FBI certainly does not recruit honest and law-abiding people only to turn around and employ them in corrupt and dishonest ways. Indeed, in contrast with the requirements placed upon many of the personnel employed by telecommunications and computer network service providers (who may have some role in implementing electronic surveillance orders), all FBI employees are specifically sworn to uphold the Constitution, obey the law, and to faithfully execute the laws of the land.

Of course, and as noted above, it is emphasized to all FBI employees that any type of illegal electronic surveillance would be a serious violation of the law—a federal felony, thereby subjecting the employee to criminal prosecution, civil liability, and termination. Further, FBI employees are made to fully understand that any unlawful surveillance will likely lead to the suppression of any and all tainted evidence and any evidence or fruits derived therefrom. In short, it is made clear that any such unlawful behavior will not be tolerated.

All FBI personnel involved in conducting electronic surveillance are thoroughly and specifically trained about the Federal electronic surveillance laws. This is particularly so for the FBI Technically Trained Agents (TTAs) who receive specialized training in the conduct of electronic surveillance, including legal instruction, at the FBI's Engineering Research Facility (ERF) in Quantico, Virginia. This training weds together the black letter law with the "hands on" technical level implementations of electronic surveillance. Moreover, FBI personnel involved in electronic surveillance are involved in ongoing consultation with attorneys from the FBI's Office of the General Counsel, the FBI Field Office's Chief Division Counsel, the Department of Justice, and the Offices of United States Attorneys.

Access to and the use of FBI electronic surveillance equipment is controlled administratively, and usually requires a trained specialist to operate it. Hence, the

large pool of FBI Special Agents and support employees never have access to, or competency in the use of, such highly-specialized pieces of surveillance equipment.

In sum, over the last 32 years, the FBI's record of properly conducting court authorized electronic surveillance is a very good one—one that we believe should command the trust of the public and the Congress.

With regard to Carnivore, it is a relatively new electronic surveillance tool, and has only been used within the last two years. Trust in the FBI's use of Carnivore, we believe, should at least in part rest upon the FBI's openness and willingness to discuss this device. Indeed, perhaps the most telling fact about Carnivore, as an electronic surveillance tool, is that in an unprecedented fashion, the FBI has shared with numerous entities in the public Carnivore's (and/or some of its technical counterparts') purpose and basic functionality—long before any concerns were raised and before any Congressional hearings were scheduled.

Ironically, the most central fact and aspect of the entire matter has gotten lost: that the FBI has spent a considerable amount of time, money, and energy in developing an electronic surveillance tool with the exclusively laudable purposes of better satisfying the Constitutional standard of particularity, the Title III and ECPA precepts of minimization, as well as the legal, privacy-based, and societal concerns associated with careful, precise, and lawful surveillance efforts.

As the Committee may be aware, the FBI has briefed a wide-ranging variety of entities: governmental attorneys, leading ISPs, leading Information Technology (IT) companies, leading telecommunications service providers, academic labs, and software manufacturers as to the functionality of the Carnivore system. Hence, if, for the sake of argument, the FBI had ever possessed any untoward intentions, in terms of using Carnivore in a stealthy, illegal, or abusive way, it certainly went about pursuing them in the wrong way. In fact, the FBI's openness with regard to Carnivore should, in and of itself, properly and reasonably instill public confidence and trust, notwithstanding that some of its detractors may disagree with some aspect of Carnivore.

Of course, with regard to Carnivore, the same strict personnel, legal, training, and security practices apply. Further, given that relatively few of these devices are even available throughout the entire FBI, those in existence are under the custody and control of but a few FBI technically-trained personnel.

Finally, the FBI, in concert with the Department, has welcomed a review of the Carnivore system. The FBI believes that when all is said and done the FBI and the Carnivore device will receive a clean bill of health, and thereby hopefully more fully instill public confidence and trust in this important and critically needed investigative tool.

*Conclusion*

In conclusion, I would like to say that over the last ten years or more, we have witnessed a continuing, steady growth in computer and Internet-related crimes, including extremely serious acts in furtherance of terrorism, espionage, infrastructure attack, as well as the more conventional serious and violent crimes, to include child pornography and exploitation. These activities which have been planned or carried out, in part, using computers and the Internet pose challenges to the U.S. law enforcement community that we dare not fail to meet. In turn, the ability of the law enforcement community to effectively investigate and prevent these serious crimes is, in part, dependent upon our ability to lawfully and effectively intercept and acquire vital evidence of these crimes, and our ability to promptly respond to these harms that so threaten the American public. As the Internet becomes more complex, so too do the challenges placed upon us to keep pace. Without the continued cooperation of our industry partners and important technological innovations such as the Carnivore system, such a task would be futile.

I look forward to working with the Committee staff to provide more information and welcome your suggestions on this important issue. I will be happy to answer any questions that you may have. Thank You.

The CHAIRMAN. Thank you so much.

Mr. Di Gregory, we will turn to you.

## STATEMENT OF KEVIN V. DI GREGORY

Mr. DI GREGORY. Thank you, Mr. Chairman. Thank you for allowing me the opportunity to testify about electronic surveillance and privacy in the digital age.

We have seen, as you have already noted, the Internet flourish over the last 10 years. In that relatively short period of time, it has created vast benefits for citizens, businesses and governments, and appears to hold boundless promise. The Internet has spurred a new economy, and many businesses have been built and people employed through Internet sales of products and services.

Others have assisted in building, maintaining and improving the Internet itself. The Internet has given people jobs, supported families and communities, and created new opportunities for commerce for America and the world. The Internet has touched our working lives, our social lives, and our family lives.

As we have seen throughout history, however, there are those who would use powerful tools like the Internet to inflict harm on others. The Internet has not escaped this historical truth. Even in the Internet's relatively short existence, we have seen a wide range of criminal use of this technology. It has been used to commit traditional crimes against an ever widening number of victims. There are also those criminals intent on attacking and disrupting computers, computer networks, and the Internet itself.

In short, although the Internet provides an unparalleled opportunity for Americans to freely express ideas and conduct business and government, it also provides a very effective means for ill-motivated persons to breach the privacy and security of others.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like death threats, extortion, fraud, and child pornography are migrating to the Internet at a startling pace. The fourth amendment and laws addressing privacy and public safety serve as a framework for law enforcement to respond to this new forum for criminal activity.

If law enforcement fails properly to respect individual privacy in its investigative techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cyber crime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime without fear of authorized government surveillance.

If we fail to make the Internet safe, people's confidence in using the Internet and in e-commerce will decline, endangering those very benefits brought about by the information age. Proper balance is the key. Despite the fervor over the unfortunately named Carnivore, the truth of the matter is that Carnivore was created to provide us with a tool to help us enforce the laws and preserve the privacy of our citizens.

To satisfy our obligations to the public to enforce the laws and preserve public safety, we use the same sorts of investigatory techniques and methods online as we do in the physical world, with the same careful attention to the strict constitutional and legal limits which apply. We must have an investigatory tool that helps us to investigate online in the same way as in the physical world, and enables us to obtain only the information we are authorized to obtain through a court order.

For example, if a man is suspected of luring children for sex, law enforcement must determine with whom the suspect is communicating. In the recent past, such communications would have been

carried out exclusively by telephone. To find out who the suspect is communicating with, law enforcement would obtain an order from a court authorizing the installation of a trap and trace and a pen register device, and either the telephone company or law enforcement would have installed the device to comply with the court's order.

Thereafter, the source and destination of the calls would have been recorded. This is information that the Supreme Court has held in *Smith* v. *Maryland* is not subject to any reasonable expectation of privacy. Given the personal nature of the information, however, Congress required the Government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to conduct its investigation in its efforts to protect the public.

Nowadays, that same suspect is more likely to operate through e-mail or other kinds of online communications. In attempting to investigate the criminal activity, law enforcement can apply to a court for an order to obtain in real time the e-mail addresses of those persons with whom the suspect is communicating through or by e-mail.

Law enforcement needs to be able to quickly identify the source and destination of such e-mails to fulfill its obligations to the victims, in particular, and to the public generally. In the event that the investigation requires viewing the content of the e-mail, even just the subject line, then law enforcement must comply with the strict internal FBI and Department guidelines and the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

When law enforcement uses a trap and trace, pen register, or a title III order in the online context, however, we have found that at times the Internet service provider has been able or even unwilling to supply the information we need. It is for that narrow set of circumstances that the FBI needs effective online investigative tools.

Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, we believe the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet. Where the service provider cannot or will not comply with a court order to reveal addressing information or content of electronic communications, law enforcement must have some mechanism to obtain that information. It must have a tool that can obtain the information authorized by the court order, and I say again only that information authorized by the court order.

The tool should be configurable so that, for example, it can be set to gather only the e-mail addresses of those persons with whom the suspect is communicating without any human being either from law enforcement or the service provider viewing the private information that is outside of the scope of the court order. Such a tool automatically reduces the data collected to only that permitted by the court, thus allowing law enforcement strictly to comply with the order and safeguarding the privacy of information outside the order.

The FBI created Carnivore to be such a tool. We have numerous mechanisms in place to prevent possible misuse of electronic surveillance tools. The fourth amendment, of course, restricts what law enforcement can do with the software, as do the statutory requirements of title III and the Electronic Communications Privacy Act. And, further, implementing orders of the courts will restrict us and will prevent possible misuse of electronic surveillance tools.

For Federal title III applications, as you know, the Justice Department imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes, and the courts. For example, before Carnivore can be used to intercept wire or electronic communications, with the limited exception of digital display pagers, the requesting investigative agency must obtain approval for the title III application from the Department of Justice.

Specifically, the Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed title III application to ensure that the interception satisfies fourth amendment requirements and is in compliance with applicable statutes and regulations. If the proposal clears the Office of Enforcement Operations, approval must generally be given then by a Deputy Assistant Attorney General in the Criminal Division. Typically, investigative agencies such as the FBI have similar but separate internal approval requirements.

If the investigative agency and the Department of Justice approve a Federal title III request, it still must, of course, be approved by the proper court using familiar but exacting standards. By statute and internal departmental regulation, the interception may last no longer than 30 days without an extension by the court. Courts, as I alluded to earlier, often impose their own additional requirements.

In addition, the remedies for violating title III or ECPA by improperly intercepting electronic communications include criminal sanctions and civil suits. For violations of the fourth amendment, of course, the remedy of suppression is also available.

We recognize that notwithstanding the limited use of the software and the many protections in place, concerns remain about the computer program Carnivore. To address those concerns, the Attorney General has asked, as you have noted, Mr. Chairman, for an independent technical review of Carnivore to evaluate whether it performs the functions it was designed to perform, and does so without any greater threat to privacy or to the smooth operation of private service providers than would be posed by any other system that allows compliance with the law related to court-ordered interceptions.

The technical reviewers will have whatever access they need to discharge their responsibilities, and their report will be made public to the maximum extent that is consistent with otherwise applicable law or contractual obligations and with preserving the continued effectiveness of the software.

The report will also be reviewed by a high-level Department panel, chaired by the Assistant Attorney General for the Justice Management Division, Mr. Stephen Colgate, and including the Attorney General's chief science and technology officer; the Department's chief privacy officer; the Assistant Director of the FBI in

charge of the Bureau's laboratory Division, Dr. Kerr; and a representative of the Department's Criminal Division. That panel will consider the positions of interested parties, such as industry and privacy groups, concerning the technical review and will report to the Attorney General.

Mr. Chairman, thank you again for allowing me this opportunity to address our efforts to fight crime on the Internet and preserve the privacy rights conferred by the fourth amendment and statutes. The need to protect the privacy of our citizens from criminals, as well as the Government, is the paramount consideration in all our activities. The public is undoubtedly concerned about their online privacy and the potential for criminals, private industry and the Government to infringe upon it.

The public is also deeply concerned, we believe, about their safety and security when exploring and using the ever-expanding reaches of the Internet. By deterring and punishing those criminals who violate individual privacy, ensuring the ability of law enforcement to fight cyber crime both promotes safety and security of Internet users and enhances user privacy. The Department of Justice stands ready to work with the members of this committee and others to achieve these important goals.

Mr. Chairman, that concludes my prepared statement. We have provided the committee with my full written statement, and thank you very much. Hopefully, later, we will be able to answer any questions you or Senator Leahy may have.

[The prepared statement of Mr. Di Gregory follows:]

PREPARED STATEMENT OF KEVIN V. DI GREGORY

Mr. Chairman and Members of the Committee, I appreciate your providing me with this opportunity to testify about the computer program "Carnivore." This Committee has previously heard from Deputy Attorney General Eric Holder and Assistant Attorney General for the Criminal Division James K. Robinson and concerning cybercrime issues. We are pleased to continue to participate in this very important dialogue today, and to address the imperative of protecting individual privacy on the Internet from unwarranted governmental intrusion, and the critical role the Department plays to ensure that the Internet is a safe and secure place for our citizens.

*Privacy and the Obligation to Provide Public Safety*

Our obligation to the public to enforce the laws is not limited to activities in the physical world; our responsibilities to the citizens to preserve their safety continues where illegal conduct is committed on-line or facilitated by the Internet. The public rightfully expects, for example, that law enforcement will investigate and prosecute child molesters who prey on children using electronic mail or other Internet communications tools.

Similarly, of course, the duty of law enforcement to preserve privacy does not end where the Internet begins. The Fourth Amendment protects the rights of our citizens as we go on-line to work, learn and explore the Internet, just as the Fourth Amendment protects rights in the physical world. The goal of the Department is long-honored and noble: we must preserve the privacy of our citizens while protecting their safety. History has taught us, and our founding fathers recognized, that our citizens' liberty cannot thrive unless we can investigate, apprehend and prosecute those who engage in criminal conduct. At the same time, however, our founding fathers abhorred the disregard and abuse of privacy by the government in England. Privacy and public safety can be at odds in certain circumstances. The founders of this nation adopted the Fourth Amendment to address those situations. Under the Fourth Amendment, the government must demonstrate probable cause to a neutral magistrate before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that less intrusive investigate steps should be permitted under a less exacting threshold. The Electronic Communications Privacy Act establishes a three-tier system by which the government can ob-

tain stored information from electronic communication service providers. In general, the government needs a search warrant to obtain the content of unretrieved communications (like e-mail), a court order to obtain transactional records, and a subpoena to obtain information identifying the subscriber. See §§ 18 U.S.C. 2701–11.

In addition, to obtain information identifying who is sending or receiving communications to or from a particular suspect, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. See 18 U.S. 3121 et seq.

Because of the privacy values it protects, the wiretap statute, 18 U.S.C. §§ 2510–22, commonly known as Title III, places a higher burden on the real-time interception of oral, wire and electronic communications than even the Fourth Amendment requires. To listen to or record communications as they are happening, law enforcement must obtain a court order unless one of the specified statutory exceptions applies. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized. The Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Rather, they provide boundaries for law enforcement, clarifying what is acceptable evidence gathering and what is not.

Often, our obligations to enforce the law and our goal to preserve privacy are in complete harmony, such as when we apprehend and prosecute a criminal who has hacked into a computer containing the confidential records of others. In those instances where there is tension, we must find a proper balance. Law enforcement has a critical role to play in preserving privacy against intrusions by others. Although the primary mission of the Department of Justice is law enforcement, Attorney General Reno and the entire Department understand and share the legitimate concerns of all Americans with regard to personal privacy. If the Internet is to thrive and citizens' confidence in the Internet is to remain high, we can abandon neither the goal of on-line privacy nor the goal of public safety.

The Department has been and will remain committed to protecting the privacy rights of individuals. We look forward to working with Congress and other concerned individuals to address these important matters in the months ahead.

*Keeping the Peace in Cyberspace*

Although the Fourth Amendment is over two centuries old, the Internet as we know it is stillin its infancy. The huge advances in communications technology over the past decade have forever altered the landscape of society worldwide. The Internet provides a new forum in which citizens can communicate, transfer information, engage in commerce, play and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly evolving technology. As has happened to every major technological advance, however, we are seeing individuals and groups use the Internet to commit crimes. As the Department has noted in the past, this nation's vulnerability to computer crime is astonishingly high and threatens not only economic prosperity, but the privacy of our citizens and our country's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are migrating to the on-line world. Crimes like death threats, extortion, fraud and child pornography have migrated with startling speed to the Internet. The Fourth Amendment and laws addressing privacy and public safety serve as the framework for law enforcement to respond to this new forum for criminal activity. If law enforcement fails properly to respect individual privacy in its investigate techniques, the public's confidence in government will be eroded, evidence will be suppressed, and criminals will elude successful prosecution. If law enforcement is too timid in responding to cybercrime, however, we will, in effect, render cyberspace a safe haven for criminals and terrorists to communicate and carry out crime, without fear of authorized government surveillance. If we fail to make the Internet safe, people's confidence in using the Internet and e-commerce will decline, endangering the very benefits brought by the Information Age. Proper balance is the key.

To meet our responsibilities to the public to enforce the laws and preserve the safety, we use the same sorts of investigative techniques and methods on-line as we do in the physical world, with the same careful attention to the strict constitutional, statutory, internal and court-ordered boundaries.

For example, if a man is suspected of luring children for sex, law enforcement must determine with whom the suspect is communicating. In the recent past, such communications would have been carried out exclusively by telephone. To find out who the suspect is communicating with, law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register"

device, and either the telephone company or law enforcement would have installed these devices to comply with the court's order. Thereafter, the source and destination of calls would have been recorded. This is information that the Supreme Court has held is not subject to any reasonable expectation of privacy. Given the personal nature of this information, however, the law requires government to obtain an order under these circumstances. In this way, privacy is protected and law enforcement is able to investigate to protect the public.

Now, that same suspect is more likely to operate through e-mail or other kinds of online communications. In attempting to investigate the criminal activity, law enforcement can apply to a court for an order to obtain in real time the e-mail addresses of those persons with whom the suspect is communicating through or by e-mail. Law enforcement needs to be able to quickly identify the source and destination of such e-mails to fulfill its obligations to the victims in particular and the public generally. In the event that the investigation requires viewing the content of the e-mail—even just the subject line—then law enforcement must comply with strict internal FBI and Department guidelines, and the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2521.

At times, Internet service providers may be unable to use their own technology to comply with court orders directing them to supply source and destination information or the content of communications. Law enforcement cannot abdicate its responsibility to protect public safety simply because technology has changed. Rather, the public rightfully expects that law enforcement will continue to be effective as criminal activity migrates to the Internet.

It is for such narrow set of circumstances that the FBI designed "Carnivore." When a criminal uses e-mail to send a kidnaping demand, to buy and sell illegal drugs or to distribute child pornography, law enforcement needs to know to whom he is sending messages and from whom he receives them. To get this information, we obtain a court order, which we serve on the appropriate service provider. Because of the nature of Internet communications, the addressing information (as opposed to the content of the communication itself) is often mixed in with other non-content data that we have no desire to gather. If the service provider can comply with the order and provide us with only the addressing information required by court order, it will do so and we will not employ any investigative tool.

Where the service provider cannot or will not comply with a court order to reveal addressing information or content of electronic communications, law enforcement must have some mechanism to obtain the information. It must have a tool that can obtain the information authorized by court order, and only that information. The tool should be configurable such that, for example, it can be set to gather only the e-mail addresses of those persons with whom the kidnapper is communicating, without allowing any human being, either from law enforcement or the service provider, to view private information outside of the scope of the court's order. Such a tool automatically reduces the data collected to only that permitted by the court, thus allowing law enforcement strictly to comply with the order, and safeguarding the privacy of information outside the order. The FBI created Carnivore to be such a tool.

We have numerous mechanisms in place to prevent possible misuse of electronic surveillance tools. The Fourth Amendment, of course, restricts what law enforcement can do with the software, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and the implementing orders of the courts.

For federal Title III applications, the Department of Justice imposes its own guidelines on top of the privacy protections provided by the Constitution, statutes and the courts. For example, before Carnivore may be used to intercept the content of communications, the requesting investigative agency must obtain approval from the Department of Justice asking a court for a Title III order. The Office of Enforcement Operations in the Criminal Division of the Department reviews each proposed Title III application to ensure that the interception satisfies the protections of the Fourth Amendment and complies with applicable statutes and regulations. Even if the proposal clears the OEO, the application cannot go to to a court without approval by a Deputy Assistant Attorney General or higher-level official in the Department. Although this requirement of high-level review is required by Title III only with regard to proposed intercepts of wire and oral communications, the Department voluntarily imposes the same level of review for proposed interceptions of electronic communications (except digital-display pagers). Typically, investigative agencies such as the Federal Bureau of Investigation have similar internal requirements, separate and apart from Constitutional, statutory or Department of Justice requirements.

If the investigative agency and the Department of Justice approve a federal Title III request, it still must, of course, be submitted to and approved by a court of proper jurisdiction. The court will evaluate the application under the Fourth Amendment and using the familiar standards of Title III. By statute, for example, the application to the court must show, through sworn affidavit, why the intercept is necessary as opposed to other less-intrusive investigative techniques. The application must also provide additional detail, including whether there have been previous interceptions of communications of the target, the identity of the target (if known), the nature and location of the communications facilities, and a description of the type of communications sought and the offenses to which the communications relate. By statute and internal Department regulation, the interception may last no longer than 30 days without an extension by the court.

Courts also often impose their own requirements. For example, many federal courts require that the investigators provide periodic reports setting forth information such as the number of communications intercepted, steps taken to minimize irrelevant traffic, and whether the interceptions have been fruitful. The court may, of course terminate the interception at any time.

The remedies for violating Title II or ECPA by improperly intercepting electronic communications can include criminal sanctions, civil suit, and for law enforcement agents, adverse employment action. For violations of the Fourth Amendment, of course, the remedy of suppression is also available.

The Justice Department and law enforcement across this nation are committed to continuing to work together and with their counterparts in other countries to develop and implement investigative strategies to successfully track, apprehend, and prosecute individuals who conduct criminal activity on the Internet. In so doing, the same privacy standards that apply in the physical world remain effective online.

As the Committee is aware, the Administration recently transmitted to Congress a legislative proposal addressing various issues relating to cyber-security. Two portions of the bill relate directly to today's discussion. First, the Administration supports raising the statutory standards for intercepting the content of electronic communications so they are the same as those for intercepting telephone calls: high-level approval, use only in cases involving certain predicate offenses that are specified by statute, and statutory suppression of evidence derived from improper intercepts. Second, the Administration bill requires federal judges to confirm that the appropriate statutory predicates have been satisfied before issuing a pen register or trap-and-trace order. Those changes would apply to the use of Carnivore, and in important respects would simply confirm by statute the policies and procedures already followed by the Department of Justice. The Administration supports a balanced updating of laws to enhance protection of both privacy and public safety, and the bill contains important provisions that would be most helpful in the ongoing fight against cyber-crime.

We recognize that, notwithstanding the limited use of the software and the many protections in place, concerns remain about the computer program. To address those concerns, the Attorney General has asked for an independent technical review of Carnivore to evaluate whether it performs the functions it was designed to perform, and does so without any greater threat to privacy or to the smooth operation of private service providers then would be posed by any other system that allows compliance with the law relating to court-ordered interceptions. The technical reviewers will have whatever access they need to discharge their responsibilities, and their report will be made public to the maximum extent that is consistent with otherwise applicable law or contractual obligations and with preserving the continued effectiveness of the software as a law-enforcement tool. The report will also be reviewed by a high-level Departmental panel, chaired by the Assistant Attorney General for the Justice Management Division and including the Attorney General's Chief Science & technology Advisory, the Department's Chief Privacy Officer, the Assistant Director of the FBI in charge of the Bureau's Laboratory Division, and me. That panel will consider the positions of interested parties, such as industry and privacy groups, concerning the technical review, and will report to the Attorney General.

Mr. Chairman, the Department of Justice takes privacy concerns seriously and takes a proactive leadership role in making cyberspace safer for all Americans. The cornerstone of our cybercrime prosecutor program is the Criminal Division's Computer Crime and Intellectual Property Section, known as CCIPS. Founded in 1991 as the Computer Crime Unit, CCIPS became a Section in 1996. CCIPS has grown from five attorneys in 1996 to nineteen today, and we need more to keep pace with the demand for their expertise. The attorneys in CCIPS work closely on computer crime cases with Assistant United States Attorneys known as "Computer and Telecommunications Coordinators," or CTC's, in U.S. Attorney's Offices around the nation. Each CTC receives special training and equipment and serves as the district's

expert on computer crime cases. CCIPS and the CTC's work together in prosecuting cases, spearheading training for local, state and federal law enforcement, working with international counterparts to address difficult international challenges, and providing legal and technical instruction to assist in the protection of this nation's critical infrastructes. CCIPS also provides its expertise to the public through its Internet website, www.cybercrime.gov. We are very proud of the work these people do and we will continue to work diligently to help stop criminals from victimizing people online.

I also note that public education is an important component of the Attorney General's strategy on combating computer crime. As she often notes, the same children who recognize that it is wrong to steal a neighbor's mail or shoplift do not seem to understand that it is equally wrong to steal a neighbor's e-mail or copy a proprietary software or music file without paying for it. To remedy this problem, the Department of Justice, together with the Information Technology Association of America (ITAA), has embarked upon a national campaign to educate and raise awareness of computer responsibility and to provide resources to empower concerned citizens. The "Cybercitizen Awareness Program" seeks to engage children, young adults, and others on the basics of critical information protection and security and on the limits of acceptable online behavior. The objectives of the program are to give children an understanding of cyberspace benefits and responsibilities, an awareness of consequences resulting from the misuse of the medium and an understanding of the personal dangers that exist on the Internet and techniques to avoid being harmed.

*Conclusion*

Mr. Chairman, thank you again for allowing me this opportunity to address our efforts to fight crime on the Internet and preserve the privacy rights conferred by the Fourth Amendment and statute. The need to protect the privacy of our citizens from criminals as well as the government, is a paramount consideration in all our activities. The public is undoubtedly concerned about their on-line privacy, and the potential for criminals, private industry, and the government to infringe upon it. The public is also deeply concerned about their safety and security when exploring and using the ever-expanding reaches of the Internet. By deterring and punishing those criminals who violate individual privacy, ensuring the ability of law enforcement to fight cyber-crime both promotes the safety and security of Internet users and enhances user privacy. The Department of Justice stands ready to work with the Members of this Committee and others to achieve these important goals.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer you questions

The CHAIRMAN. Thank you so much.

Mr. Cerf, we will take your testimony at this time.

## STATEMENT OF VINTON G. CERF

Mr. CERF. Thank you very much, Mr. Chairman. It is a pleasure to be here. Good morning, Senator Leahy. It is a pleasure to see you again as well.

I am here representing the Internet Society, although for purposes of identification, the chairman is quite correct, I also serve as senior vice president at WorldCom for Internet Architecture and Technology.

For many, many years I worked on the Internet, and for a long time many of you know that getting the Internet protocol out there was an important goal. So I even had a T-shirt made to commemorative. It reads "IP on everything," and that is what I have been doing for a long time.

However, the FBI is now confronted with a serious problem because now that the Internet protocol is going everywhere, everyone wants to put all new applications on top of it. So, as a result, we have Internet telephony and television and radio and e-mail and World Wide Web. So now I have another T-shirt that says "Everything on IP," although one could read this "IP Under Everything," which is another way of thinking about it.

That is the problem confronting the FBI today, is that these communications——

Senator LEAHY. You have made sure this will be the one thing that we will remember from this hearing. [Laughter.]

The CHAIRMAN. If you had any guts, you would have worn those T-shirts.

Senator LEAHY. Don't encourage him, Mr. Chairman. [Laughter.]

Mr. CERF. I don't know if I want to go there any further. Thank you, Mr. Chairman.

The CHAIRMAN. But I have met a lot of your associates in this business and they wear T-shirts.

Mr. CERF. My purpose today is entirely technical. I am not prepared to, and I don't even consider myself competent to speak to the policy side of these questions. But I do want to make some attempt to explain how difficult it is to achieve what the Carnivore system tries to do, so let me remind you a little bit about the Internet.

First of all, think of the packets that flow through it as if they are postcards. Postcards don't necessarily stay in order as they go through the Postal Service. This is true on the Internet as well. They get lost. In fact, in the Internet world sometimes we have to duplicate them in order to get reliable delivery to the far end.

The other thing which is characteristic of the Internet is that it works with computers with a lot of software in them and the software is structured in layers. So the lowest layer is the Internet protocol layer, but there are layers on top of that, each one depending on the ones below it for performing the functions that achieve reliability or implement things like electronic mail.

So as an example of what happens when someone is sending e-mail from place to place on the Net, let me start with an example. This is a simple little e-mail from Tom Bell to Vinton Cerf, and we will pretend like this is the original message that—for people back there, there you are. That is the original message that is prepared by the sender. But by the time the FBI gets a chance to look at it through the Carnivore System, what they will see is, in fact, not this message, but rather a series of envelopes which I have numbered 1, 2, 3 and 4.

They may not see them in this order. They may see them in the order 1, 3, 2 and 4, depending on where the Carnivore system is actually located in the network. If it is close to the source of the messages, then it may actually see them in order. But because of retransmissions and other things, you may still see them out of order.

What is more interesting is that when you open up one of these Internet packets to see what is in inside, what you discover is only a piece of the e-mail that started out as one whole message. And, in fact, you may not be able to tell from looking inside who it is from or where it is going because not all of the message is there. All of the header information that says "to Vint Cerf" and "from Tom Bell" may not be visible in the particular packet that you happen to have detected.

So it is a big challenge for the Carnivore system to have its parameters set to filter out only those packets that have information in them that is useful to the surveillance. In fact, because of the

way this system has been implemented, it is looking at each packet one at a time. It doesn't assemble them together and then look at them. It sees each one as if it were through a keyhole.

As a result, if you don't see enough information in here, you will have discard it because you won't, in fact, be able to identify it as useful to the surveillance. So they actually lose quite a bit of information. They don't see as much as they would if they were trying to assemble everything. The result is that they will see, for example, a subset of all the messages I may send and receive to someone as e-mail.

If, on the other hand, they are permitted to record all of the information because the court order says they can see everything, then after they have captured these packets, you can put them back together and examine the complete messages and extract from them the part of the information that you are permitted to extract.

Now, in order to do that properly, you are going to actually see everything in the message and you will have to filter out the part that says "to" and "from" because the physical way in which you pull these things together allows you to see the entire thing if you are permitted to see all of the traffic. If you are only permitted to see the packets, then you will just see those messages that happen to have in them enough information to identify this as an e-mail from Vint Cerf to a particular target.

So I would argue that, technically speaking, the Carnivore system sees less than would be absolutely allowed in the case that they are only permitted to see the "to" and "from" addresses. If, however, they are permitted to see everything, they can, in fact, see everything and then have to filter that out and discard the portion of the traffic which is not relevant.

Then the other thing that I want to point out, then, is that the placement of the Carnivore system is pretty crucial to all of this. I would like to make an analogy, if I could.

Let's imagine for the sake of argument that our postal services are done with post office boxes, that we have no home addresses, we have no home delivery of postal mail. We all have to go to our post office boxes in order to retrieve our messages. The Internet behaves a lot like that because the mail systems are like post offices that contain post office boxes.

The FBI's problem is that if they were trying to observe the traffic going from one party to another, from one post box to another, the only thing that they can see is traffic going between post offices, not post office boxes. All they get to see in the Internet packet is something that says this is the Annandale post office and this is the Springfield post office, and that is all the traffic they can see. You have to open it up and look deeper to figure out from which post office box it is going.

That is why there is such concern that you may be seeing more than you are allowed to see. But my understanding of the way the Carnivore configuration is set up is it is very limited in its ability to capture packets with respect to the "to" and "from" addresses or the equivalent post office box addresses.

So the last thing I would like to point out in this discussion is that the technology that allows people to protect privacy makes life even harder for the FBI in the course of doing this surveillance be-

cause if you use what is called end-to-end cryptography—and there is plenty of that now available both domestically and internationally—the object that they had to look at that was inside this packet to figure out the "to" and "from" addresses of the mail could be encrypted. As a result, the target may not be visible. So this makes the job of the FBI even more difficult in the event that end-to-end cryptography is used.

I see that I have overstayed my welcome, but let me stop there and say that the FBI's implementation of Carnivore attempts, in my estimation, to limit the amount of information that is being captured, but it is very, very hard to do that successfully, and the cryptography makes their job even more difficult.

I would be happy to answer any questions that may come about as a consequence of further discussion at this point. Thank you very much.

[The prepared statement of Mr. Cerf follows:]

PREPARED STATEMENT OF DR. VINTON G. CERF

Mr. Chairman, my name is Vinton Cerf. I am present on behalf of the Internet Society; a non-profit educational and research institution devoted to the continued evolution and spread of the Internet on a global basis. For purposes of identification only, I am also senior vice present at WorldCom where I am responsible for Internet Architecture and Technology, but my testimony today is on behalf of the Internet Society where I serve as a trustee. I served a the founding president of the Society from 1992 to 1995 and have served on its board of trustees since 1992. In 1997, President Clinton awarded the National Medal of Technology to me and to Dr. Robert E. Kahn for our roles in the invention and implementation of the Internet.

The purpose of my testimony today is technical. I hope to provide you, Mr. Chairman and the other members of the committee with a sense for how the Internet works and how the FBI Carnivore system operates within the architectural framework of the Internet. I thank you for this opportunity to share these technical ideas with you and I hope that they will prove to be useful as the committee considers the policy implications of the Carnivore technology.

Let me begin by offering a simple analogy that has proven to be helpful in the past to explain some basic principles by which the Internet functions. To begin with, the Internet is not a single network but, rather a network of networks interlinked on a global scale. The precise figure is not known but there are probably on the order of 300,000 networks, worldwide, interconnected to form the Internet. There are an estimated 100 million service computers on the Internet and approximately 330 million users. These figures do not include laptops, desktops, mobile telephones and Internet-enabled appliances that are on the Internet on a sporadic basis. The technology used by the Internet to switch data among the computers on the network is called "packet switching" and is quite different from the technology used to support conventional voice telephony services.

In the traditional voice telephone network, the end devices (telephones and fax machines, typically) "dial" each other up and the network forms end-to-end electronic circuits the pair of communicating devices. The connection remains in place until one or the other device "hangs up" or, as occasionally happens, the telephone system accidentally disconnects the parties. As far back as 1961, it was recognized by a few individuals that a very different mode of operation would be appropriate to link networks of communicating computers. That technology eventually became known as "packet switching."

In principle, computers communicate with each other in a "bursty" fashion. That is, they compute for a while and then emit a burst of information, then go back to computing. This is particularly true in time-shared machines that serve many users concurrently. Each user feels as if he or she has the computer resource all to himself or herself, but in fact the computer is so much faster than the user, it is possible to appear to be a dedicated resource when, in fact, the machine serves each user in turn. The service rate is fast enough that, most of the time, the sharing is not noticed by users. Of course, if the resources of the serving computer are over-subscribed, users may in fact find themselves waiting for service.

A "packet" is a brief computer message of perhaps a few thousands bits (up to a thousand or so characters) containing some indication of the source of the message

and the destination in addition to the content. The best analogy that I have been able to come up with so far is to compare a packets to ordinary post cards.

Each postcard has a "from:" address and a "to:" address. So does each Internet packet, but the packet addresses are Internet addresses that are something like telephone numbers. A postcard has a finite amount of content, and so does an Internet packet. When you put a postcard into the postal system, it is picked up from the postbox and transported to the destination, passing through one or more post offices and carried by truck, plane, train, boat or even on foot on its way to the destination. Similarly, an Internet packet may be carried over optical fiber, telephone twisted pair copper lines, coaxial television cables, point to point radio or satellite.

When you put a postcard into the postal system, there is no guarantee that it will come out! The same is true of an Internet packet! When you put two postcards into the postal system there is not guarantee that they will come out in the same order they went in, even if addressed to the same destination. The same is true of Internet packets. The Internet does one other thing that the Post Office does not do. Occasionally it will deliver duplicate packets to the destination—that's not a feature of the U.S. Postal Service, as far as I am aware.

As postcards are routed through the postal service, they are forwarded from one post office to another until they reach the destination post office after which they are delivered to the target address. Devices called "routers" serve the same function in the Internet as post offices in the sense that they take in packets and forward them from router to router until the destination is reached.

The Internet uses what is called the Internet Protocol to forward packets between computers in what is, effectively, a kind of computer post card service. A "protocol" is simply a set of conventions and formats used to achieve communications. The postal service dictates that addresses take a certain format and occupy certain places in a postcard—Internet packets have their own format and procedures for being injected into and taken out of the Internet. The standards and procedures used by the Internet are essentially developed by a body called the Internet Engineering Task Force and the architecture of the Internet is looked after by the Internet Architecture Board. These two groups operate under the auspices of the Internet Society.

There is more, however, to Internet than the basic Internet Protocol (the electronic postcard system). The Internet architecture is called a "layered" system because there are actually several layers of procedures. Each higher level procedure or protocol relies on the lower level protocol(s) to perform basic functions. One sometimes hears or reads the expression "TCP/IP" in association with the Internet. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. These are the two basic protocols that Bob Kahn and I began working on in 1973 and they form the basis of the Internet as we know it today. The Internet Protocol was designed to operate on top of virtually any digital transmission and switching system and, in fact, I have had a T-shirt made to emphasize this notion. The T-shirt reads "IP on Everything"!

The Internet Protocol, as you should now realize, does not guarantee the reliability of the packets it transports, nor does it assure ordering, or the path over which the packets are transported. But there are a great many applications that require these features, and more, to function successfully. The Transmission Control Protocol (TCP) was designed to make up for the deficiencies of the Internet Protocol by keeping things in sequence, recovering from loss and filtering out duplicates.

To see how TCP does this, another analogy is useful. Let us suppose that Senator Hatch wants to send a book to Senator Leahy by means of a postal service that can only carry postcards. How would he set about accomplishing this task? He would first have to remove pages of the book and cut them up to fit on post cards. Then he would notice that not every postcard had a page number so Senator Leahy might have difficulty piecing the post cards back in the right order, so he would decide to number each page. Then he would remember that not all the postcards would necessarily reach Senator Leahy, so he would keep copies of them in case duplicates had to be sent. Then he would wonder how he would know when to send duplicates. Senator Leahy might then think of a good idea: he would occasionally send a postcard back to Senator Hatch to say that he'd gotten every postcard up to, say, number 402. But then Senator Leahy would remember that his postcard might not reach Senator Hatch. At this point, both Senators would conclude that Senator Hatch will have to have some kind of time-out, after which he would begin sending copies of postcards that had not been acknowledged, until he receives confirming postcards from Senator Leahy. Finally, Senator Leahy would remind Senator Hatch that his mailbox can hold only a finite number of postcards. If the book Senator Hatch wants to send turns into 1000 postcards but Senator Leahy's mailbox can only hold 200 at a time, both Senators might conclude that if by a miracle, the US Post Office

actually delivered all 1000 postcards at the same time, some of them might get lost if they didn't fit into Senator Leahy's mailbox. This would lead them to conclude that they should agree that Senator Hatch won't send more than 200 postcards at a time and would not have more than that "outstanding" until Senator Leahy has confirmed their receipt.

Well, in principle, that is the way the TCP protocol turns the simpler Internet Protocol into a reliable, sequenced and flow-controlled service. This isn't quite the way in which Bob Kahn and I developed the TCP but it isn't very far away from the basic reasoning!

At this point, it is possible to explain how the FBI's Carnivore observation system makes use of the Internet and to outline the limitations of its operation. In this brief exposition, I will assume that the Senate Judiciary Committee members are well-acquainted with the legal basis on which the FBI occasionally is granted permission to intercept domestic communications in the course of enforcing the laws of the United States. As I understand the law, such surveillance is carried out only after the conduct of judicial proceedings intended to assure that any such surveillance is documented and justified. In the past, such surveillance has been associated with the interception of telephone-based communications but just like the rest of the citizens of the United States, law-breakers are making increasing use of electronic mail and other kinds of Internet-based communication, including such things as chat rooms, in the conduct of their activities.

The FBI, in recognition of this trend, has developed new methods of observing computer-based communications and one such system has been named "Carnivore."

To understand what Carnivore is and how it works, we need to take one more foray into the world of analogies. I mentioned earlier that the Internet architecture is "layered"—that is, it consists of a number of different protocols each one layered on top of the other and each layer relying on the one below it for certain functions. For example, the Internet Protocol layer that performs the forwarding of packets relies on the lower levels to actually transport the bits of information that make up each packet. The TCP layer relies on the Internet Protocol to deliver packets, and TCP makes sure they are put back in order and retransmitted if any are lost. The electronic mail service has its own protocol (called Simple Mail Transport Protocol or SMTP) and that service makes use of TCP. It turns email messages into TCP streams of data that are broken up into Internet packets and sent by varying paths toward the destination where the packets are reassembled first into a sequenced stream of information by TCP and parsed into messages again by the SMTP.

The layered architecture is mirrored in the implementation of the software that uses the protocols. The email client software that is used to compose email produces the text of messages that look something like:

Date: Tue, 05 Sep 2000 19:27:05 +0100
From: <tom.bell@wcom.co.uk>
Subject: Thank you
To: <Vinton.G.Cerf@wcom.com>

Dear Sir,

I would like to thank you for the very useful information that you included in reply to my request.

Sharon Bell

This text is to be sent to the electronic mail box of user Vinton.G.Cerf on the computer on the Internet that has the "domain name" wcom.com ("To: *Vinton.G.Cerf@wom.com*"). However, the email composition program knows that the TCP service does not know where computer "wcom.com" is on the Internet. So it "looks up" the name of this computer in a distributed directory called the Domain Name System, and discovers that the Internet address of this computer is: 204.176.69.71. You can think of this as a kind of Internet telephone number for purposes of this exercise.

The email composition program creates a kind of envelope that it addresses to 204.176.69.71, puts a return address of the Internet address of the computer that is sending the email, say 170.127.34.16, and places the email message in the envelope. In spirit, the envelope looks something like:

From: 170.127.34.16
To: 204.176.69.71
(Attention: For the SMTP service via the TCP program)

The TCP program takes this envelope and cuts it into pieces (including the contents!!) and sends the pieces in smaller envelopes that are addressed, again by analogy:

From: 170.127.34.16
To: 204.176.69.71
(Attention: for the TCP Program via the Internet Protocol)

These smaller envelopes function like the Internet Postcards that were introduced in the earlier part of this testimony. They are sent through the series of computers we call "routers" that serve in the same fashion as post offices, to forward the traffic by potentially different paths to the destination.

At the destination computer ("wcom.com"), the process is reversed and the small Internet Protocol envelopes are opened, the contents reassembled by the TCP program into a message and the result is handled to the SMTP receiving program. That program puts the received message away in the mailbox associated with Vinton.G.Cerf on the wcom.com computer. Later, when user Vinton.G.Cerf runs the email reading and composition program he will be able to see the message and to respond to it.

The important concept to take away from these preliminary remarks are:

1. The concept of packets ("postcards");
2. The idea that packets do not always stay in order, may be lost, and may even travel on distinct paths through the Internet;
3. The understanding that there are tens of thousands of Internet Service Providers around the world operating hundreds of thousands of networks that make up the Internet and that traffic may flow through a number of such networks as it flows from source to destination; and
4. The concept of layering and the notion that each layer "envelopes" the information generated by the layer above and that anyone observing traffic on a particular circuit that carries Internet packets will actually be observing pieces of messages (or files or bits of digitized sound) carried in the small Internet Protocol envelopes.

The Carnivore system is a computer that tries to observe the traffic (Internet packets) flowing on a circuit within the Internet. Its objective is to try to find only those packets that may be relevant to an ongoing investigation and to ignore theirs (both for legal reasons and simply to deal with the potentially enormous flow of traffic that may require filtering). It's a bit like trying to find a particular shrimp in the intake of a baleen whale!

The physical location of the Carnivore computer is important. If it is observing traffic somewhere in the middle of the Internet, it may not even see all the packets that correspond to a particular exchange between computers or even a complete transmission from one computer to another. One could try to place Carnivore computers at different locations in the Internet, hoping to catch all the requisite traffic but in fact, the only way to achieve reasonable success is to locate the Carnivore computer so it can observe all the traffic going to and from the computer under observation. That may mean locating the Carnivore computer where it can see everything going into and out of the location of the subject of surveillance, watching all traffic going to and from the subject's laptop or desktop, or locating the Carnivore computer at the Internet Service Provider who serves that subject and placing it in such a way that the traffic going to and from the subject's email server computer can be observed.

Furthermove, since the Carnivore looks at each individual Internet packet and does not perform reassembly of the packets in real time, there are some limits to what the software can do to recognize relevant traffic. It can plainly see the "to:" and "from" Internet address of the Internet packets (e.g., 170.127.34.16). It may not be able to see the "To: *Vinton.G.Cerf@wcom.com*" in every packet because this is NOT contained in every Internet packet. One has to reassemble the massage at the SMTP level of protocol (two layers above the Internet Protocol) to be assured of seeing this. But this may require that all the packets or most of the Internet packers carrying the email be intercepted and this may or may not be assured, depending on the rate at which these Internet packets must be examined by Carnivore and whether most of the packets are actually present on the circuit being monitored.

The Carnivore operators have the ability to be very precise about which Internet addresses are of interest and can ignore all other traffic. They can tell which protocols are being carried in these Internet packets (TCP, among others, including steaming protocols based on the so-called User Datagram Protocol). If the contents of the IP packers are NOT encrypted they will be able to see for what layer of protocol above TCP or UDP the traffic is intended so they could distinguish email (SMTP) from file transfer (FTP) from World Wide Web traffic (HTTP).

If the contents of the TCP traffic is encrypted, as it often is with the World Wide Web for financial transactions, it is not possible in real time for the Carnivore system to see any deeper into the traffic than to know that it is World Wide Web traf-

fic. The encryption is often quite robust, using up to 128 bit keys and strong cryptographic codes.

Some of the more recent standards for security for the Internet even introduce cryptography at the level of the Internet Packet so that it contents are encrypted end to end. Both the current version 4 IP protocol and the more recent version 6IP protocol have provisions for such encryption using the so-called IPSEC standard.

The Carnivore system has been configured so that it is possible to limit the amount of information retrieved from any particular packet so that, for example, the only information that might be collected is the source or designation address of the Internet packet and none of the content. It is may understanding that the Carnivore implements have gone to considerable length to build in mechanisms to restrict traffic capture to conform to the limitations that any particular court-approved surveillance may impose.

In summary, the Carnivore system is fairly basic system that must do its work by observing single packets of traffic at a time and attempt to determine based on a limited set of parameters whether this packet is relevant to the desired surveillance. It is not a system that is capable of observing all the traffic flowing through the Internet at once nor even all the traffic flowing through any one reasonably-sized Internet Service Provider's system.

It is also important to note that this system is not unlike commercially available tools that help network operators debug problems in the network by analyzing the protocols that are in use and observing the states that these protocols go through in the course of an interaction. These protocol analyzers generally do not capture packet contents but rather work their way up through the "envelopes" to understand the sequences of events that may be causing a problem for the users or operators of a particular ISP or a collection of them.

Readers of this testimony should remember that reasoning by analogy can sometimes lead to incorrect conclusions. I hope the use of analogy has been educational and not misleading, but precision answers about Carnivore should be sought from the engineers who have designed it, and not drawn solely on the basis of the analogies I have tried to use to explain the concepts behind its operation.

Thank you.

The CHAIRMAN. Thank you, Mr. Cerf.

Professor O'Neill, we will turn to you.

## STATEMENT OF MICHAEL O'NEILL

Mr. O'NEILL. Chairman Hatch, Senator Leahy, I welcome this opportunity to testify regarding a topic that should obviously be of great interest to us all, and that is, namely, the appropriate way in which law enforcement interests should be balanced against what Justice Douglas once called our fundamental right to be left alone.

I think I would also like to just take a second and just thank Mr. Cerf, as well, for helping to design something that has helped break the grip that TV formerly held on my life.

I do not wish to belabor points that have already been made, nor am I here to make claims that Carnivore is going to eat the Constitution or that if we fail to deploy it that crime will somehow run rampant. I think it is safe to say that none of us in this room likely wishes to live in a police state, nor do we particularly wish to live in a state of anarchy either.

We live now in a time of profound technological change, and the communications revolution has been a part of that change. Change, however, is not without its costs. Privacy, one of the fundamental rights underpinning our society, is presently under assault as perhaps never before, and not only by the government, but also by business interests.

On the other side of the equation, however, criminal enterprises have been increasingly willing to utilize technological innovations to achieve their own ends and thereby threaten our personal secu-

rity. While we may stand at the brink of a new world in terms of information, however, we still have old rules, rules that have served to guide us well for over 200 years and that will continue to serve as a guide for us for our understanding and ultimately controlling the many technological transformations surrounding us.

With that in mind, I would like to address two fundamental issues. One, is Carnivore, at least as I understand the software to operate, compatible with the requirements of the Fourth Amendment? And, two, what role should Congress play in ensuring that both significant privacy and security interests are addressed?

Our Constitution presupposes that, as citizens, we enjoy a sphere of action free from governmental interference. To this end, the Drafters of the Bill of Rights had the foresight to include as a fundamental guarantee to protect the right of the people in their persons, houses, papers and effects against unreasonable searches and seizures. The term "unreasonable" is really key here. We are protected, at least from the government, only against those searches that are per se unreasonable.

The fourth amendment's reasonableness requirement has an important application to today's debate; namely, after all, what is deemed unreasonable is entirely and ultimately a social construct. It is, at the end of the day, for the people to decide what is and is not a reasonable intrusion into their private affairs.

The difficulty I have in coming before you today is that I am not at all confident that I know what is reasonable in this particular context. If polled, most individuals, I suspect, would assume and likely prefer that their e-mails be every bit as secure, if not more so, than standard snail mail.

The evolution of the privacy/security struggle has been well defined in the development of fourth amendment law. In *Olmstead* v. *United States*, a 1928 case that was sort of the harbinger of the wiretap and ultimately the electronic surveillance revolution, the Supreme Court considered whether warrantless wiretapping violated the fourth amendment. The Court found ultimately no constitutional violation because surveillance was accomplished without intruding upon the defendant's physical property.

Justice Brandeis, however, penned a thoughtful dissent in which he observed that constitutional principles were undermined to the extent that the Court focused exclusively on the means of communication. He reasoned that the Constitution must be interpreted with technological advancements in mind to preserve fundamental rights and liberties.

Foreshadowing those advancements, he warned that, quote, "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered at in the closet."

Now, the Court ultimately adopted Justice Brandeis' view toward wiretapping. In *Katz* v. *United States*, it declared that the Fourth Amendment protects people, not places, and held wiretapping permissible only after the issuance of a valid warrant. This decision expressly overruled *Olmstead*, replacing the previous focus on the means of the communication with an appreciation for the fact that the communication itself was the source of the constitutional right.

The Court subsequently revisited this area in *Maryland* v. *Smith*, a 1979 case that you have heard the executive branch relied upon to justify its claim that there is no expectation of privacy in an Internet address. In *Smith*, however, the Court reasoned that there is no legitimate expectation of privacy in a number being dialed on a telephone.

It is important to understand, however, that the Court found that individuals do not have this expectation of privacy because pen registers themselves do not acquire the contents of communications. The technology in question was limited to this single function. This neat categorization, however, may not apply to technologies such as Carnivore which may have far greater information-gathering abilities.

A URL, for example, can disclose specific pages visited, sites visited, or even items that have been purchased or browsed on the Internet. And as people move more of their lives online, a list of e-mails sent or Web sites visited can provide a very detailed dossier of activities, all available without the heightened standards of a wiretap or even a regular fourth amendment warrant. This is far more akin to walking into somebody's office and snooping around in their file cabinet than it is to standing on the street corner and writing down their physical address.

Given the wealth of information obtainable by means of an Internet address, perhaps it is time to rethink our privacy expectations online. Indeed, I think it is increasingly difficult to say that you don't have an expectation of privacy in information that is in the hands of a third party. If the vision of an open, PC-less Internet world is to come to pass, it will be the case that much of our lives will be in the hands of third parties.

Indeed, currently I do all of my banking and manage my meager stock portfolio all on the Internet. All of this information is contained online. To simply treat the "to" and "from" lines in e-mails as though they were the phone numbers that you dial out on just doesn't make sense anymore.

Moreover, the physical ease with which information is obtained becomes important. Ordinarily, a search is limited by a number of physical properties. You have to be on site, you have certain time limitations. Internet searches, however, make the retrieval of vital data, even otherwise public data, far more routine. For example, while property tax assessment records are public, people generally had to take the time and hassle to schlep on down to the court house to retrieve them.

In a matter of minutes, however, just the other night I was able to retrieve fairly easily Chairman Hatch's property tax records. And basically now I know what the value of his current assessed land is. I know how many bedrooms he has in his house.

The CHAIRMAN. I wouldn't mind knowing that myself. [Laughter.]

Mr. O'NEILL. Well, sir, I would be happy afterwards—I won't submit this for the record, but I will be happy to give it to you after we have finished.

Now, again, that is public information, information that is always obtainable at the court house. But the mere fact that late last night, in a process of about, I don't know, maybe half a dozen keystrokes and a matter of about five minutes or so I could obtain all

this information, should give us at least some cause for pause about what we are getting ourselves into.

Mr. CERF. You are not making a threat, are you?

Mr. O'NEILL. Oh, not at all.

Mr. CERF. OK; I am just checking.

Mr. O'NEILL. I used to work for him, so I felt it was okay.

Mr. CERF. OK.

Mr. O'NEILL. But I did the same thing for Senator Leahy as well.

Senator LEAHY. I was thinking. I mentioned to the chairman that he must have paid you too much if you have got a stock portfolio.

Mr. O'NEILL. Senator, I was smart; I married a doctor.

The CHAIRMAN. That is a typical Democrat comment—failing to recognize the importance of the Internet and all of these other great programs that we have.

Senator LEAHY. We Democrats try to keep down the cost of Government. That is why.

The CHAIRMAN. We hadn't noticed that. [Laughter.]

Mr. O'NEILL. I will try to remain silent on that issue.

Similarly, I think another problem that we have to address is we don't even know how certain Fourth Amendment doctrines will apply in this field and to a device like Carnivore which, although it may have physical limitations and may, in fact, be limited in its application, may be configured or updated in ways that we are not necessarily aware of. It may have the potential of reading e-mail or looking at other addresses that people visit.

The plain view doctrine, for example, permits, among other things, law enforcement officers to seize items in their plain view when they are executing a warrant. Well, if we allow law enforcement to filter nonspecific pieces of mail, does that mean that they can seize anything else that they may happen to find of a criminal nature which is not necessarily contained within the plain language of the warrant? These are among the fundamental issues that we will ultimately need to address as the law struggles to cope with technological advancements.

Now, I don't want to go too far over the red light here, but I have ten fairly specific recommendations that I would consider that perhaps Congress ought to consider in terms of deciding and securing our privacy online. I will actually submit those for the record and I won't belabor those points now.

But I think that this hearing is an important first step in looking at these important privacy issues as they come before us, and one simple suggestion that I might make is that government, specifically the Congress of the United States, should set itself up as the primary protector of people's liberty and security interests. And it is not a bad idea at all, I think, either to place within the Intelligence Committee or perhaps one of the other committees of jurisdiction careful congressional oversight of precisely the types of information and the sources of information that the Department of Justice is seeking to obtain when it does things such as Carnivore to search out people's private information.

But, again, I will submit those and the remainder of my remarks for the record. I again thank you for this opportunity to testify and look forward to answering any questions you may have later.

The CHAIRMAN. Well, thank you, professor. I think the FBI and Justice are going to want to look at your ten suggestions those fairly carefully because there are some very interesting suggestions there.

[The prepared statement of Mr. O'Neill follows:]

PREPARED STATEMENT OF MICHAEL O'NEILL

Chairman Hatch, Senator Leahy, and members of the Committee, I welcome this opportunity to testify regarding a topic that should be of great interest to us all, namely the appropriate way in which law enforcement interests should be balanced against what Justice Douglas once called our fundamental right "to left alone." [*U.S. v. Davis,* 328 U.S. 582 (1946).

I do not wish to belabor points that have already been made. Nor am I here to make claims that Carnivore will eat the Constitution, or that if we fail to deploy it, crime will run rampant. I think it is safe to say that none of us in this room likely wishes to live in a police state, nor, however, do we desire to live in a state of anarchy.

We live in a time of profound technological change, and the communications revolution has been a vital part of that change. Change, however, is not without its costs. Privacy, one of the fundamental rights underpinning our society, is presently under assault as perhaps never before. On the other side of the equation, however, criminal enterprises have been increasingly willing to utilize technological innovations to achieve their own ends and thereby threaten our personal security.

While we may stand at the brink of a new world in terms of information, however, we still have old rules, rules that have served us well for over 200 years, and that continue to serve as a guide to understanding, and controlling, the transformations surrounding us.

With that in mind, I would like to address two fundamental issues: (1) is Carnivore, at least as I understand the software to operate, compatible with the Fourth Amendment? And (2) What role should Congress play in ensuring that both significant privacy and security concerns are addressed?

Our constitution presupposes that as citizens, we enjoy a sphere of action free from governmental interference. to this end, Drafters of the Bill of Rights had the foresight to include as a fundamental guarantee to protect "the right of the people * * * in their persons, houses, papers, and effects, against *unreasonable,* searches and seizures." The term "unreasonable" is the key here * * * we are only protected against those searches that are unreasonable. The Fourth Amendment's reasonableness requirement has an important application to today's debate. After all, what is deemed "unreasonable" is ultimately a social construct * * * it is at the end of the day for the people to decide what is and is not a reasonable intrusion into their private affairs.

The difficulty I have in coming before you today is that I am not at all confident that I know what is "reasonable" in this particular context. If polled, most individuals, I suspect, would assume, and likely prefer, that their e-mails be every bit as secure, if not more so, than their snail mail.

The evolution of the privacy/security struggle has been well-defined in the development of Fourth Amendment law. In *Olmstead* v. *United States* (1928), the Supreme Court considered whether warrantless wiretapping violated the Fourth Amendment. The Court found no constitutional violation because the surveillance was accomplished without intruding on the defendant's physical property. Justice Brandeis, however, penned a thoughtful dissent in which he observed that constitutional principles were undermined to the extent the Court focused exclusively on the *means* of communication. He reasoned that the Constitution must be interpreted with technological advancements in mind to preserve fundamental rights. Foreshadowing those advancements, he warned that: "Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet."

The Court ultimately adopted Justice Brandeis' view toward wiretapping. In *Katz* v. *United States*, it declared that the Fourth Amendment "protects people, not places" and held wiretapping permissible only after the issuance of a valid warrant. This decision expressly overruled Olmstead, replacing the previous focus on the *means* of communication with an appreciation of the *fact* of communication as the source of the constitutional right.

The Court subsequently revisited this area in *Maryland* v. *Smith* (1979), a case the executive branch has often relied upon to justify its claim that there is no expectation of privacy in an internet address. In Smith, the Court reasoned that there

is no legitimate expectation of privacy in a number being dialed on the phone. It is important to understand, however, that the Court found that individuals do not have a reasonable expectation of privacy in such information because "pen registers do not acquire the contents of communications. *Smith* v. *Maryland*, 442 U.S. 735, 742 (1979). The technology in question was limited to this single function. This neat categorization may not apply to technologies such as Carnivore, however, which may have far greater information gathering abilities.

An URL, for example, can disclose specific pages visited, sites visited, or even items purchased or browsed. And as people move more of their lives online, a list of e-mails sent or web sites visited can provide a very detailed dossier of activities—all available without the heightened protections of a wiretap or even a standard Fourth Amendment warrant. This is much more akin to walking into someone's office and snooping around in their file cabinet than it is to standing on the street corner and writing down their address. Given the wealth of information obtainable by means of an internet address, perhaps it is time to re-think our privacy expectations on-line. Indeed, I think it is increasingly difficult to say that you don't have an expectation of privacy in information that is in the hands of a third party. If the vision of an open, pc-less internet world is to come to pass, it will be the case that our entire lives will be in the hands of third parties. To treat the "To" and "From" lines in e-mails as though they were just the same as the phone numbers that you dial makes little sense.

Moreover, the physical ease with which information is obtained becomes more important. Ordinarily, a search is limited by a number of physical properties. Internet "searches," however, make the retrieval of vital data, even otherwise public data, far more routine. For example, while property tax assessment records are public, people generally had to take the time, and hassle, to go to a court house to retrieve them. In a matter of minutes, however, I was able to easily retrieve [hold up records] Chairman Hatch's property tax data. Don't worry, I won't disclose it * * * but I do know how many bedrooms, bathrooms, and fireplaces you have in your home * * *!

Similarly, we don't know exactly how certain Fourth Amendment doctrines will apply to a device, such as Carnivore, that has the potential of reading personal e-mail, as well as, via the internet address, entering the individual's hard drive and scoping it out. The plain view doctrine, for example, permits (among other things) law enforcement officers to seize items in their "plain view" when they are executing a warrant. Well, if we allow law enforcement to filter non-specific pieces of mail, does that mean they can seize anything they happen to find? These are among the fundamental issues that will need to be addressed as the law struggles to cope with technological advancements.

### WHAT QUESTIONS OUGHT CONGRESS BE ASKING?

Law enforcement has pointed out that the law must be changed to preserve its mission to prevent and punish crime, while the civil liberties community has warned of grave dangers to personal privacy and the Fourth Amendment. Although each group may emphasize different aspects of the problem, each agrees that the law must be updated to keep pace with technological change. Remarkably, the 1986 Electronic Communications Privacy Act was the last significant update to the privacy standards of the electronic surveillance laws. Significant changes have occurred since then, including—the development of the Internet; data convergence; the creation of wireless systems; and the movement of information out of people's homes and offices onto networks controlled by third parties. As a result of these developments, more information is being held and communicated in configurations where it is in the hands of third parties and not afforded the full protections of the Fourth Amendment.

The following steps might therefore be in order.

(1) With respect to Carnivore itself, Congress ought to obtain briefings, classified, if necessary, to get a better understanding of what Carnivore is designed to do and how it does it, and whether there exists potential for abuse.

(2) Congress ought to determine what the statutory authorization for Carnivore is and whether law enforcement has the authority to insist that a service provider install Carnivore.

(3) If implemented in some fashion, Congress should require that statistics be maintained by the Justice Department, and that these so-called "audit trails" be routinely provided for legislative oversight.

(4) Congress should seek to learn whether Carnivore can easily be defeated by encryption software or E.A. Poe type purloined letter schemes.

More broadly,

(5) Hearings out to be conducted to determine whether all internet trap and trace orders should be issued only on the basis of a judicial finding that reasonable cause exists to believe that a target has or is about to commit a crime;

(6) The executive branch ought to be required to provide consumers with notice whenever the government obtains information about their Internet transactions;

(7) Specific statistical reports for Internet trap orders similar to the reports required under Title III ought to be require;

(8) Congress should explicitly provide that Internet queries, e-mail subject lines, URL's of sites visited and other information which provides more than the equivalent of a dialed number cannot be disclosed without a probably cause order.

(9) Congress should consider requiring notice and an opportunity for defendants to object when civil subpoenas seek personal information about Internet usage.

(10) Finally, Congress ought to provide enhanced protection for information on networks: including the establishment of probably cause for seizure without prior notice, and providing a meaningful opportunity to object to subpoena access.

At bottom, I would urge a cautious, thoughtful approach when it comes to expanding surveillance capabilities. The conflict between increased security and enhanced privacy protection is not easily resolvable, nor will it likely ever be. But Congress ought to seize the moment to ensure that robust debate occurs before law enforcement's powers are enhanced, and regardless of how the balance is struck.

The CHAIRMAN. Mr. Dempsey, we will turn to you.

## STATEMENT OF JAMES X. DEMPSEY

Mr. DEMPSEY. Mr. Chairman, Senator Leahy, good morning. Thank you again for holding this hearing and for giving me the opportunity to testify. I am at a certain point, I think, going to use just one overhead, if I could, but in order not to delay things I will talk while they are setting up the projector.

I think I wanted to start out by responding to one of the points that the FBI and the Justice Department make which they regularly make and I think which needs to be regularly rebutted or balanced, and that is the point about the use of the Internet by criminals.

Undoubtedly, criminals do use the Internet, but I think if you look at the facts over the past two or three years, it is clear that the Justice Department and the FBI have been extremely successful in using the new technology to track criminals online and to make cases, including some cases that they probably couldn't have made in the offline environment.

Online surveillance and tracking led to the arrest of the Phonemasters, who were stealing and selling credit card numbers worldwide; Solar Sunrise culprits, one of whom was tracked down to Israel; an intruder on NASA computers who was arrested and prosecuted in Canada; the thieves who broke into the Citibank computers and who were tracked and arrested in Russia; Ardita, who was tracked down electronically to Argentina; the creator of the Melissa virus. All of these people were tracked online using this very technology.

Innocent Images is another example of where FBI agents are able to pretend online to be young girls or to be pedophiles and to legally entrap people. In the Emulex case that you referred to, Mr. Chairman, investigators said that they learned within hours of the stock's plunge where the computer was located that the perpetrator had used, and they obviously have arrested that person.

Back in August, two Kazhaks were arrested in a cyber extortion case. Their communications went from Kazhakstan to London and to the target in New York, which was Bloomberg. Yet, they were traced back using this very technology, and in response to that

Bloomberg pointed out these arrests show that our law enforcement agencies can find, catch, and bring criminals to justice online. Criminals believe that they have a totally anonymous presence on the Internet. They believe that they can intimidate companies. This operation shows that they do not have that kind of anonymity.

So I think we need to recognize—and Professor O'Neill in his online search showed us how easy it is to find so much information. And I think, if anything, what we need to do is to not abandon the traditional rules that we have had to protect privacy but, in fact, to strengthen those rules in the face of the surveillance and investigative power of this new technology.

Now, turning specifically to Carnivore, the first problem that we have with Carnivore is that we don't know really what it is and how it works. It is something that is now totally controlled by the FBI. It is a black box. They have refused to share publicly the details of that, and they have put out a request for proposal to conduct an independent review, which is a good idea even if it were conducted outside of the public light.

But the FBI and the Justice Department have set out for this independent review so many restrictions and they have put such burdens on anybody who would sign up to do that, such secrecy burdens, that a lot of the good people are backing out of that, are backing out, it seems, from competing for that. And it does call into question, with the kinds of restrictions the FBI has set, whether they will be able to get the best people to do that review.

Today, in USA Today Online, there is a story by Will Roger in which he states that MIT, Purdue University, Dartmouth, the University of Michigan, and the Super Computer Center at the University of California at San Diego have all indicated their reluctance to participate in that review, given the constraints that the FBI has posed in terms of pre-review, and so on.

The second issue I would like to emphasize is that Carnivore is fundamentally inconsistent with the way that wiretaps have been done in the past, and fundamentally inconsistent with the understandings of this committee repeatedly over the years.

Traditionally, we have not allowed the FBI into the networks, into the switching systems and into the property of ISP's. A major, major problem with Carnivore, and I think a lot of the source for the concern about it, is that it is a black box that the FBI imposes on the ISP.

Now, this committee in 1986, when it was adopting ECPA—and Senator Leahy was the prime author of that legislation in the Senate—this committee in its report on ECPA emphasized telephone company customers have a reasonable expectation, traditionally enhanced by telephone company practice and policies, that their company will not become, in effect, a branch of government law enforcement.

The committee went on to say that they understand that the practice has been that the telephone company premises are not used for wiretap activity. And the committee actually directed—I don't know if it happened—the Justice Department in its wiretap manual to state that there would be a statement there in the manual that U.S. attorneys should not attempt to compel any company to make its premises available for wiretap activity.

And the committee in 1986 asked for notification if there was a change in that policy and if the Justice Department did decide to try to compel carriers to make their premises available and what is Carnivore to basically latch this software and hardware into the network.

Again, in CALEA, in 1994, this committee reemphasized that, and there is section 105 in CALEA which specifically says that telephone companies—CALEA does not apply to the ISP's, but it is the principle here that the committee cared about quite strongly. CALEA says that a telecommunications service provider shall design its system so that a wiretap is activated within the switching premises and controlled by telephone company personnel, not by law enforcement personnel, precisely because this committee was concerned about the problem of remote FBI access to the actual guts of the network of a service provider.

I think a lot of the concerns that people have with Carnivore would be mitigated if the software and the ability to control the software were placed in the hands of the service providers rather than held and controlled by the FBI.

Now, I wanted to talk a little bit about the way——

The CHAIRMAN. How can you trust the service providers any more than you trust the FBI?

Mr. DEMPSEY. Well, I think what we have to do is we have to have a system of checks and balances; that is, we have to have some buffer or barrier between the customer and the Government.

The CHAIRMAN. It is one thing for the telephone companies to have control over how the transmission is made. It is another thing to have the ISP's—who have tremendous software capabilities themselves in control of the transmissions.

Mr. DEMPSEY. Well, many of the ISP's already perform and comply with court orders, as Dr. Kerr made clear. Many ISP's do not need Carnivore, do not accept Carnivore, and do comply on their own with the court orders.

Mr. CERF. May I? I have just two comments to make. One observation is that the Carnivore equipment is a passive device. In other words, it doesn't actively enter into the control stream or anything like that. It simply taps information. In fact, as was pointed out by the FBI, it is prohibited technically from transmitting anything into the Net. So in that sense, that is helpful because it is passive.

I would certainly debate the advisability of having the ISP personnel setting the parameters and managing the capture of e-mail-related information. In fact, I would be more concerned about——

The CHAIRMAN. I think it is a different situation than phone companies.

Mr. CERF. Sir?

The CHAIRMAN. I think it is a different situation than phone companies—much broader.

Mr. CERF. Well, even going and setting parameters, let alone inventing software, the side effect of having the ISP personnel do that is that you may not get protection of the evidence in the evidentiary chain. You may get exposures of information that are not legal. The FBI operators are well aware of those restrictions, but the ISP operators are probably not.

So I am not sure that I would be as comfortable as you sound like.

Mr. DEMPSEY. We have headed pretty far down the road in allowing ISP's who can perform to do so. Of course, the FBI can go back and say you didn't give us everything that we wanted, and that process can go forward.

In the telephone realm, the way we are heading in CALEA is that it will be an intercept function that is activated by carrier, pursuant to an order——

The CHAIRMAN. Yes, but collected by the FBI.

Mr. DEMPSEY [continuing]. To isolate and identify what is the stream of communications. In the Internet, it is harder because we do not have a circuit-switched system.

Mr. CERF. You actually have to work your way up in those layers of protocol in order to see what is going on. In fact, the simple analogy here, these little letters, is that if you watch a stream going from a customer's personal computer going into or coming from the Internet, it could contain a variety of information all at the same time. There could be some voice communication, there could be video, there could be e-mail, there could be a World Wide Web exchange, all of this happening at once. And the stream of packets going by in these little envelopes have to be opened up and examined in order to figure out which one is it.

The CHAIRMAN. One of the questions I am going to have is how does the FBI protect this information from the ISP collecting it? That is a question that I think——

Senator LEAHY. But the ISP could look at it any time they wanted anyway.

The CHAIRMAN. Yes, but they may not know what they are looking for, where the FBI knows what they are looking for.

Mr. CERF. In order for the ISP to perform the same function that the Carnivore system does, they would have to essentially build the same kind of software that the FBI is using and configure it to capture the portion of the stream that is of interest. In a sense, they would have to reproduce all of the technology that goes into Carnivore.

There are systems like that. They are called sniffers, but they are not as sophisticated, in fact, at restricting the information that is captured. Moreover, there are none of the safeguards that the Carnivore system has for keeping track of who did what.

Senator LEAHY. Well, are you saying by that then that no ISP system today, whether they have sniffers or not, can match Carnivore? And if so, does that mean the FBI are going to have to say, well, we have always got to use our own system because you are not good enough?

Mr. CERF. What I am saying is that the devices that are available that are used to help debug problems on the network that will allow you to crawl up and down in the so-called layers can capture everything. The problem is that that is not what the FBI wants to do. What it wants to do is to capture only that part that is——

Senator LEAHY. But that goes, then, to my particular point. Are you saying that nobody today can duplicate what the FBI is doing? Thus, the FBI whenever they have one of these court orders is going to have to use their own?

I see Ms. Stansell-Gamm shaking her head no, but I just——

Mr. CERF. What I am trying to say is that the technology exists to capture information off the Net. An ISP has that capability because these are off-the-shelf devices. The implementation of Carnivore is intended to constrain the way that capture is done and the ISP doesn't have the particular motivation to go and do that, to invest in all that.

The CHAIRMAN. They don't have the same interests as the FBI. They are not going to be doing that.

Mr. Cerf. That is correct.

The CHAIRMAN. Well, let me finish with Mr. Dempsey and then go to Professor Rosen.

Mr. CERF. I am sorry I interrupted you.

Mr. DEMPSEY. If I could, to round out this dialog, I think that there is an answer to the dilemma here, and that is to take the Carnivore software and make it available to the ISP's so that they know what it is, know how it works. They can configure it, they can set the parameters as ordered by the court order. And then you do have that protection in the middle that you don't have the FBI, in essence, taking control of a part of a network or inserting itself into the network. I think that a lot of the concerns about Carnivore would be mitigated if this software technology were disclosed and made available to ISPs.

The CHAIRMAN. Well, let's go to Professor Rosen, but I have a lot of problems with that because then you have a nonlaw enforcement agency—a private company—being able to do whatever they want to do with people's knowledge and people's information.

You have made some interesting suggestions. I want to really look at those because I don't know what the answer is here. All I can say is that I don't want to have *1984* in 2004, but we are already there. With nanotechnology coming up now—if you read Kurtzweil's book—it is enough to scare the living daylights out of every one of us. And if you read Bill Joy's article, I mean, my gosh, it is mind-boggling.

Senator LEAHY. But, Orrin, they can do this now.

The CHAIRMAN. Yes, I know.

Senator LEAHY. The ISP's can do this now anyway.

The CHAIRMAN. They can do it now anyway.

Senator LEAHY. They can step through and get most of this now. They might have a different reason, a different purpose, but they can do it.

The CHAIRMAN. But they don't need to have the assistance of the FBI to do it.

Mr. DEMPSEY. If I could, Mr. Chairman, just before you go to Professor Rosen—and we can go back to this later in the questions—I just wanted to lay out two other areas that I think merit discussion here, one of which is the question of whether Carnivore constitutes a search for fourth amendment purposes and an interception for title III purposes. I believe that, at least as the FBI has explained it on their Website, Carnivore does constitute a search and seizure for constitutional purposes and an interception for title III purposes.

Finally, I would just like to say that once again we are back to the question of how do you translate the wiretap laws to the Inter-

net. And Professor O'Neill, I think, referred to this quite well, but by developing Carnivore and by controlling and programming Carnivore and putting it out there, the FBI has basically decided that question technologically by saying that Carnivore can collect, under a pen register order, e-mail "to" and "from" addresses and other Internet addressing and routing information without ever finishing a debate which we started back here, I think, in May before this committee, which is the question of what should be the legal standards for application of pen registers to this very different medium of the Internet.

So with that, I will conclude. Thank you, Mr. Chairman.

[The prepared statement and attachments of Mr. Dempsey follow:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Mr. Chairman, and members of the Committee, thank you for calling this hearing and giving CDT* the opportunity to testify on the FBI's "Carnivore" initiative and its implications for Fourth Amendment privacy protections in the digital age.

*Summary*

We can all appreciate that new communications technologies pose challenges to law enforcement agencies carrying out important duties. But as a black box controlled by the FBI and inserted into the network of an Internet service provider to search through thousands or millions of messages, including those of innocent people, Carnivore is not the right solution. It is not consistent with the way that electronic surveillance was conducted in the past. It is not consistent with the Fourth Amendment nor with the Supreme Court's image in the *Katz* and *Berger* decisions of how electronic surveillance could permissibly be conducted. It is not consistent with the federal wiretap statute, Title III. And it is not consistent with CALEA. The FBI has to find a better way to conduct surveillance of Internet communications, one that does not entail taking control of a portion of the network of a service provider and that does not entail a general search through the communications of innocent persons.

In order to moot the serious questions about Carnivore's legality, the FBI should immediately cease insisting that it be installed outside the control of Internet service providers (ISPs). Instead, the FBI should immediately begin making the technology of Carnivore available—including the source code and the right to modify it—to any ISP that needs it to comply with a surveillance order. (Most ISPs don't need it.) If any ISP needs to adopt Carnivore or something like it, the ISP should control its own network, isolating and delivering to the government only what the government is entitled to intercept, and thus serving as a buffer between the government and the communications of their innocent customers. This would reinstitute the kind of checks and balances we depend on to preserve our rights.

Looking more broadly, Carnivore is the latest in a series of wake-up calls about the perils facing personal privacy in the digital age. Carnivore illustrates the extend to which the FBI claims the authority to actually control the design or functioning of communications networks.[1] Yet the deployment of Carnivore and other design or functional mandates for surveillance creates new and largely unappreciated threats to the security of communications. Moreover, even apart from FBI efforts to control the technology, it is clear that, despite the ways in which the newer digital technologies are harder to tap, on balance the government is acquiring far more surveillance powers as a result of the digital revolution: Market-driven changes in the technology and the ways we use it mean that we are generating more electronic in-

*The Center for Democracy and Technology is a non-profit, public interest organization dedicated to promoting civil liberties and democratic value on the Internet. Our core goals include ensuring that the Constitution's protections extend to the Internet and other new media. 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 issue.

[1] For other examples, see Neil King Jr. and David S. Cloud, Hang-Ups: Global Phone Deals Face Scrutiny from New Source: the FBI, Wall Street Journal, August 24, 2000, at A1. The implementation of CALEA has been one long struggle over the FBI's insistence on dictating very precise surveillance features to the telephone industry. See United States Telecomm Assoc. v. FCC, No. 99–1442 (D.C. Cir Aug. 15, 2000).

formation than ever before about our lives and making it available on networks and computers where it can be readily obtained by the government. Law enforcement agencies are not loosing ground—they are gaining surveillance and tracking capabilities by leaps and bounds. For all of these reasons, Carnivore highlights the need for Congress to enact greater privacy protections in the outdated statutory framework.

Among the specific points we would like to make about Carnivore:

• *The first problem with Carnivore is that we do not know how it works.* There is little understanding of how Carnivore searches are limited, and little chance for judicial or public oversight. Such a situation is ripe for mistake or misuse. The government should embrace an open source model allowing public scrutiny of Carnivore's design. Unfortunately, the "independent review" promised by the Justice Department at this point is so circumscribed and under such control of the FBI and the Department that it holds little promise of giving Congress, industry or the public reliable answers.

• *So long as Carnivore is a black box owned and controlled by the government, its forced installation in the network of an ISP means that, in essence, the government takes control of part of the ISP's network.* ISPs should control their own networks. Installing a closed Carnivore system outside of ISP control introduces new risks to the security of these networks. ISPs are in the best position to respond to court orders in a fashion that protects user privacy.

• *As far as we can tell, Carnivore searches more information than the government is legally entitled to search. Indeed, based on current description. Carnivore, when controlled by the FBI, has to be characterized as an unconstitutional governal search and an interception in violation of Title III.* If Carnivore is used as a pen register under the pen register statute as currently interpreted by the DOJ, it is likely that it searches (and intercepts, in Title III terms) content of the target. Even worse, whether used under the pen register order or a Title III probable cause order, it searches and intercepts the communications of innocent persons outside the scope of any properly issued Title III order.

• *Carnivore's use as a pen registers has pre-judged—in fact has surrendered to Executive Branch discretion and ex parte legal proceedings—the important public policy question of what data should the government collect about Internet transactions under the weak privacy standard of the pen register statute.* Without explicit statutory language, the Justice Department is asserting that it can use the rubber-stamp pen register authority to collect information from the Internet that is much more revealing than the information collected by pen registers from telephone lines. There seems to be a growing consensus that the low legal standard authorizing their use should be raised for plain old telephones. But if the government is to collect on the Internet transactional information more personally revealing than that collected on telephone lines, then it would seem that an intermediate standard must be developed for Internet transactional data.

*Context: Privacy and Surveillance in the Internet Age*

The Internet has already demonstrated its potential to promote democracy, spur economic growth, and enhance human development. Individuals, civil society, businesses and governments are all rushing to use the Internet for work, activism, education, social services, human contact, artistic expression and consumerism. The Internet has become a necessity in most workplaces and a fixture in most schools and libraries. Soon, it may converge with the television and wireless phones, and thereby become nearly ubiquitous.

Every day, Americans use the Internet to access and transfer vast amounts of private data. Financial statements, medical records, and information about our children—once kept on paper and secure in a home or office—now travel through the network. Electronic mail, online reading and shopping habits, business transactions and Web surfing can reveal detailed profiles of people's lives. And as more and more of our lives are conducted online and more and more personal information is transmitted and stored electronically, the result has been a massive increase in the amount of sensitive data available to government investigators.

While the Justice Department frequently emphasizes the ways in which digital technologies pose new challenges to law enforcement, the fact is that the digital revolution has been a boon to government surveillance and information collection. 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 percent. Computer files are a rich source of evidence: In a single case last year, the FBI seized enough computer evidence to nearly fill the Library of Congress twice. As most people sense with growing unease, everywhere we go on the Internet we leave digital fingerprints, which can be tracked by marketers and government agen-

cies alike. The FBI in its budget request for FY 2001 sought additional funds to "data mine" these public and private sources of digital information for their intelligence value.

*Wiretapping the Internet*

Our legal framework for electronic surveillance was developed in an era of circuit-switched telephone networks, where it was relatively easy to isolate the communications of a particular target to the exclusion of the communications of innocent persons, and where it was relatively easy to distinguish between transactional data, which was limited and not very revealing, and Constitutionally-protected content. Even at the time CALEA (the Communications Assistance for Law Enforcement Act) was adopted in 1994, the telephone system, while going digital, was still largely based on a circuit-switched architecture, and CALEA assumed that central telephone company switches, if loaded with special software, would provide ready access to the communications and call-identifying information of surveillance subjects. This Committee, in drafting CALEA, wisely excluded the Internet from CALEA specifically because those technical assumptions did not apply to the packetized, decentralized Internet.

By design, the Internet's architecture is not like that of the phone system. It is not centralized. It does not dedicate a channel or circuit to one conversation. It does not have permanent addresses. But surely these technological differences do not mean that we can abandon the principles of the fourth Amendment. As the D.C. Circuit recently made clear in the CALEA appeal, the mere fact that government agencies are encountering a new technology does not give them the authority to redefine the rules of interception, even where the government promises it will not record or use the information it is not entitled to. Instead, we must find ways to ensure that the fundamental distinctions of the law are maintained, and where they cannot be, the government must meet the higher, not the lower, legal standard. "Wiretapping" the Internet may require greater oversight and protection. If pen registers on the Internet reveal more than the "numbers dialed" they once provided for telephones, then the standard must be higher than the standard for telephone pen registers. And we must recognize that the government's desire to translate every current telephone surveillance capability into the Internet world (with a kind of 100% guaranteed success rate never really available with traditional telephone surveillance) would require a new technical architecture for the Internet with huge security risks.

It is in this context that the FBI's Carnivore initiative must be viewed.

*Questions about Carnivore*

Carnivore reportedly serves at least two functions. Installed at an ISP, it monitors communications on the ISP network and records messages sent or received by a targeted user. This is presumably designed to effectuate an electronic "wiretap" order served on an ISP. Carnivore can reportedly also isolate the origin and destination of all communications to and from a particular ISP customer. This is presumably designed to satisfy what law enforcement claims is the Internet equivalent of "pen register" and "trap and trace" orders, which in the telephone context provide digits dialed and incoming phone numbers. (Note that there are fundamental questions about what information pen register and trap and trace orders should collect in the Internet context.)

There are many unanswered questions about Carnivore:

How does Carnivore isolate and record only the information that the government is legally entitled to collect under a particular wiretap or pen register order? Carnivore has the potential to capture the content of communications even when a pen register order would limit collection to addressing information. Indeed, as we explain below, getting the addressing information the government claims it is entitled to often requires capturing and analyzing content. Does Carnivore avoid that? Moreover, since Carnivore operates on a network link, it has the potential to capture the traffic of customers who are not the subjects of an order. For example, Internet Protocol (IP) addresses may be used to identify the communications of a target. But in many systems such addresses are dynamically allocated (meaning that the same address will be assigned to many users sequentially, and a given user will not have the same address from day to day or hour to hour), making it quite easy to monitor the wrong user.

Is Carnivore itself a secure system? Can it be compromised? Does it provide secure audit trails, and is it tamper resistant? Is it true that Carnivore installed on an ISP's system can be remotely accessed and reprogrammed by the FBI? If Carnivore, an eavesdropping device with access to a vast stream of traffic independent

of any ISP control, were itself somehow compromised, the damage to privacy and security could be tremendous.

The technical community has developed a method to improve trust in complex systems: Open source review. Review of the source code and design specifications by a community of experts might reveal mistakes, bugs, or security holes unknown to the FBI. Such mistakes are quite common in the design of complex technical systems. Open source review of Carnivore's hardware, software, and technical design is essential to ensuring that Carnivore does not exceed its legal authority. It would also seem necessary for defense lawyers and judges to test in the adversarial process the reliability of evidence it generates.

Undoubtedly, the FBI will initially argue that revealing source code will compromise the effectiveness of Carnivore. If true, one must question the general security and usefulness of a system that can be so easily circumvented by anyone with knowledge of its operation.

The Department of Justice has promised to contract for an "independent review" of Carnivore. Unfortunately, the review has been wrapped in conditions and controls that undermine its credibility and seem to be discouraging the best experts from participating. Two in particular are especially troubling: (1) The contract documents for the review specify that the government will retain control over what portions of the reviewers' comments are released to the public. The government says that it will release as much as possible, consistent with contractual obligations and "preserving the effectiveness of Carnivore." This would seem to preclude release of conclusions about the vulnerability or effectiveness of Carnivore. Since the FBI has claimed that its contractual obligations preclude it from disclosing even the name of the company that built Carnivore, that could be another huge justification for censoring the contractor's report. (2) The implications of this are compounded by the blanket non-disclosure agreement that contractor personnel would be required to sign, in which they would promise not to disclose to anyone anything they learned in the course of their review without FBI permission. Under the agreement, sensitive information is defined as "any and all information received from the FBI" and "any and all other information associated with the Carnivore device and system." This gag order would mean that persons who now can talk about Carnivore based on their general understanding of it would be permanently silence if they participated in the review.

*In a Departure from Tradition and Best Practice, Carnivore Is Not Controlled by ISPs*

Even were there open review of Carnivore's system, installation of a "black box" out of an ISP's control creates new privacy and security risks. The parameters for how Carnivore is used once installed are likely to be extremely important. Such parameters could control who the targets are, how they are identified, and what information is collected about them. Yet with Carnivore, ISPs appear to have no control over how the system operates. Such a system provides no checks on its use, and is an invitation for misuse or mistake. Indeed, we understand that the FBI retains the sole right to alter how Carnivore operates when it is in place, and that the FBI can do so remotely, without the knowledge or cooperation of the service provider.

Carnivore is a radical departure from the way interceptions have traditionally been performed. In the world of telephone wiretaps, phone companies are extremely reluctant to allow law enforcement officials into their switching facilities. In the past, and up through the present time, telephone companies have been adamant that the would activate any interception from within their central offices. (Companies would allow law enforcement agents to activate intercepts from access points on their outside plant, like neighborhood or apartment building junction boxes, but that type of access is disappearing.) The reasons were both privacy and security.

In 1994, Congress confirmed that this principle was an important additional check on abuse. So section 105 of CALEA expressly provides that wiretaps shall be activated and controlled by telephone company personnnel:

> A telecommunications service provided shall ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier * * * 47 U.S.C. 1004, Pub. L. 103–414, section 105.

CALEA does not apply to ISPs (and should not be extended to ISPs), but Carnivore is a radical departure from the principle that service providers must keep government agents out of their systems.

ISPs themselves are in the best position to comply with lawful orders for electronic surveillance. ISPs have a dual duty, to both produce information for law enforcement and to protect the privacy of their customers by only revealing such information where required by lawful order. Moreover, ISPs are in the best position to understand their own networks and the most effective ways of complying with lawful orders. They are also in the best position to understand potential implications or threats from installation of a Carnivore device.

*Carnivore Performs an Unconstitutional General Search and an Illegal Intercept Under Title III*

Carnivore operates very differently from an ordinary wiretap or pen register. In the telephone world, it has always been possible to isolate a pair of wires or a channel or circuit that is dedicated to a targeted individual's communication. The Supreme Court's approval of wiretapping under the Fourth Amendment was based on the understanding that the government would be accessing only the communications on a particularly identified line (the "facility," in Title III terms). All of the Court's concern about ensuring that on that particularly identified line the government only intercepted communications that involved specified criminal conduct would be rendered absurd if the government could search the lines of many subscribers. See *Berger* v. *New York,* 388 U.S. 41, 58–60 (1967); *Katz* v. *United States,* 389 U.S. 347, 355–56 (1967).

According to published accounts, including information on the FBI's Web site, http://www.fbi.gov/programs/carnivore/carnlrgmap.htm, Carnivore operates by monitoring (according to the FBI's description, redirecting and copying) all traffic on the network link where it is installed. Carnivore searches through all this traffic. (A copy of the FBI's description is attached to this testimony.) In theory, Carnivore then only records data appropriate to the order under which it operates—i.e., data relating to the target of an order, or even narrower information pertaining to pen register or trap and trace orders.

Nevertheless, in Fourth Amendment terms, Carnivore, as it has been described, is conducting a "search" of all the communications on the network segment to which it is attached, including the traffic of innocent persons. That is, even if Carnivore functions as promised and only records the traffic of the target, it is *searching* through the email of many innocent persons—it is conducting an unconstitutional general search. The ISP redirects to Carnivore a stream of packets from many different customers. Carnivore filters those packets. That is a search. The fact that Carnivore is automated and that no human ever reads innocent messages does not make it any less of a search. The use of machines to carry out searches does not make them any less a search for Constitutional purposes.

In Title III terms, it also seems clear that what Carnivore does is an "intercept." As the Second Circuit states, "It seems clear that when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time. * * * Redirection presupposes interception." *United States* v. *Rodriguez,* 968 F.2d 130 (2nd Cir. 1992), cert. denied, 113 S.Ct 139, 140, 663 (19992). See also *United States* v. *Denman,* 100 F.3d 399, 403 (5th Cir. 1996), cert denied, 117 S. Ct 1256 (1997); *United States* v. *Tavarex,* 40 F.3d 1136 (10th Cir. 1994); *United States* v. *Nelson,* 837 F.2d 1519, 1527 (11th Cir. 1988), reh'g denied en banc, 845 F.2d 1032 (1988), cert denied, 488 U.S. (1988). Thus, use of Carnivore under control of the FBI is an illegal interception of the redirected communications of innocent subscribers.

*Pen Registers Do Not Translate Neatly Onto the Internet*

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 orginiating number" for incoming calls. 18 U.S.C. §3121 et seq. The Supreme Court has held that the numbers collected by a pen register on a telephone line reveal so little about a person's communication that they are not constitutionally protected. *Smith* v. *Maryland,* 442 U.S. 735 (1979). The Court has stated, "Neither the surpost 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 registers." *United States* v. *New York Tel. Co.,* 434 U.S. 159, 167 (1977). (While the information is not constitutionally protected, it is sensitive, and as CDT and others have noted, the standard for pen registers in the telephone world is now too low, since even phone numbers dialed can draw a profile of a person's life.)

Carnivore's apparent attempt to extend "pen registers" and "trap and trace" orders to the Internet is not a simple matter. Access to Internet transactional data is not clearly supported by the pen register statute, which refers to the collection only of "numbers dialed" on the "telephone line" to which the device is attached.

Moreover, Internet origin and destination addresses can be far more revealing than the Supreme Court contemplated in *Smith* v. *Maryland* and *New York Tel. Co.*

Extending the use of pen registers to new telephone devices and services—such as pagers, or numbers dialed after a call is completed—has been the subject of debate[2] and was one of the issues in the CALEA lawsuit where the Court of Appeals reversed the FCC.[3] But Carnivore is indicative of a whole new and problematic expansion of the pen register to the Internet. See CDT memo dated April 4, 2000, "Amending the Pen Register and Trap and Trace Statute in response to Recent Internet Denial of Service Attacks, and to Establish Meaningful Privacy Protections," *http://www.cdt.org/security/000404amending.shtml.*

The first question is what Internet transactional data may be collected and under what standard. It is one thing if the FBI were using the pen register authority only to collect IP addresses (provided, of course, that the isolation were done by the service provider rather than by an FBI-controlled Carnivore). In the packet-switched Internet, the literal "destination" of an intercepted message is often the Internet Protocol (IP) address of the link on which it is observed. This information is found in the header of a packet. So is the Ethernet address it is being sent to on a local network. If the government is seeking just IP or Ethernet address information, it can find it in the header of a packet, which is easily separated form the content.

But if by destination the government means the "To:" line of an e-mail message, that is often within the packet's content payload, and as the DC Circuit recently made clear, intercepting addressing information that is commingled with content requires authority to intercept content. *United States Telecomm Assoc.* v. *FCC* (Aug., 12, 2000).

In an effort to illustrate this point, I have attached some packets we "sniffed" off our own DCT network. Example 1 shows a packet for a visit to Chairman Hatch's web page. The header of the packet includes the source the destination IP addresses. In this case, the source IP address 207.2263.15 is a computer at CDT and the destination 199.95.76.12 is the U.S. Senate web server. (If you type 199.95.76.12 into your browser after http://, it takes you to the Senate home page just as if you had typed www.senate.gov.) So the header, which can be easily separated from the content payload, would provide information that might be similar to the information that a pen register would provide on a person at CDT who called 224–3121, the Senate switchboard.

However, if the FBI wanted to know what precise page I was viewing, they would need to reach into the content (TCP data) portion of the packet. There they would find that I had asked for ("Get") a copy of /-hatch/greeting.ram. Anybody typing that into a browser would find that I had downloaded the video greeting on the Chairman's web page. Thus, they would know the precise content of my Web viewing.

In other cases, where law enforcement is apparently seeking origin and destination addresses that are more than link IP addresses, they will be forced to analyze the contents of packets. For example, attached in Example 2 are three sample IP packet "sniffed" as they went from CDT's network to our ISP. The packets are part of an e-mail message from me to Makan Delrahim, a member of the Committee staff. The header of each packet shows the IP addresses of the packet's origin (a computer at CDT) and destination (our ISP's mail server, which will next send the packet to the Senate mail server). To find out to whom the e-mail is addressed to, one would need to read and analyze the contents of specific packets. Is Carnivore able to pick out only the one packet that contains only the "To:" information and the one packet that contains only the "From:" information? It would be nice to have some assurance other than the FBI's say-so.

The e-mail addresses in the To and From lines are much more revealing than "numbers dialed" in that they are associated with specific persons. In the case of a Web site, the URL can disclose specific pages visited, books browsed, or items purchases. And as people move more of their lives online, a list of e-mail recipients by name or web sites visited can provide a very detailed dossier of activities—all available without the heightened protections of a wiretap or even a standard Fourth Amendment warrant. For example, attached in Example 3 is a sample IP packet showing a search for a book on the Barnes and Noble web site. Again, the IP address information is available in the header; the URL in the body of the message reveals information about what books the user is looking at—here, books on prostate cancer. (A subsequent URL might indicate that the person actually bought the book.) Taken together, a collection of such "destination" information could generate

---

[2] *See,. e.g., Brown* v. *Waddell,* 50 F.3d 285, 290–91 (4th Cir. 1995) (refusing to classify a digital display pager clone as a pen register).

[3] See *United States Telecomm Assoc.* v. *FCC,* No. 99–1442 (D.C. Cir Aug. 15, 2000).

a revealing list of a person's interests and activities. In this way, Internet transactional information is more revealing than telephone transactional data.

CDT has long urged, and there seems to be a consensus, that Congress should raise the standards for use of pen registers across the board. Under the current standards, a judge "shall" approve any request signed by a prosecutor certifying that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C.§§3122–23. This is low standard of proof, similar to that for a subpoena, and judges are given no discretion in the granting of orders. Pen registers are executed with neither public nor judicial oversight: in contrast to wiretap orders, there is no requirement that the government ever report back to the authorizing judge on the results of a pen register and no requirement of notice to the targets of pen registers. Unlike wiretaps, there are no national reporting reqirements on the use of pen registers. The Justice Department reports on its own use, but this does not include numerous federal, state and local use.

The Carnivore debate raises Fourth Amendment questions for pen registers online. Courts have found that consumers have no "expectation of privacy" in the digits they dial on a telephone.[4] Given the revealing nature of Internet transactional information, it would seem that users do have a reasonable expectation of privacy in the URLs of Web sites they visit and the email addresses of those with whom they communicate, such that an intermediate standard is necessary for collecting certain Internet transactional data. See 18 U.S.C. 2703(d) and H.R. 5018, the "Electronic Communications Privacy Act of 2000," introduced by Reps. Canady and Hutchinson.

*Reinvigorating the Fourth Amendment in Cyberspace*

On May 25, 2000, I testified before this Committee about the ways in which the statutory and constitutional framework governing electronic surveillance has been outpaced by technological change. *http://www.senate.gov/-judiciary/52520jxd.htm.*

To update the privacy laws, and respond specifically to Carnivore, Congress could start with the following issues:

- Increase the standard for pen registers across the board.
- Define and limit what Internet transactional information can be disclosed to the government and under what standard.
- 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 those required by 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, and a meaningful opportunity to object for subpoena access.

The recent White House announcement[5] on privacy and surveillance adopts some of these proposals. Extension of the wiretapping exclusionary protections to electronic interceptions is a particularly welcome step. Increasing the standard for pen registers is an improvement, but will not be sufficient if such orders are applied broadly (i.e., include URLs) to the Internet. On the other hand, the proposed expansion of the Computer Fraud and Abuse Act criminalizes an unnecessarily broad range of activities online. The proposal fails to address the need for heightened protections for private data held in the hands of third parties. And there are other changes buried in the proposal that we are still analyzing. CDT is prepared to work with Congress and the Justice Department to continue to flesh out the needed privacy enhancements, and to convene DPSWG as a forum for discussion and consensus building on these issues.

---

[4] *See Smith* v. *Maryland,* 442 U.S. 735 (1979). The Court's reasoning relied in part on its understanding that "pen registers do not acquire the contents of communications."

[5] *See* Ted Bridis, Updating of Wiretap Law for E-Mail Age is Urged by the Clinton Administration, Wall Street Journal., July 18, 2000, at A3.

*Conclusion*

The Carnivore system requires greater public scrutiny. It should be controlled by the ISPs. More broadly, it speaks to the need for modernization of our surveillance laws and greater privacy protections to counteract the real threats to privacy online.

Protecting national security and public safety in this new digital age is a major challenge and priority for our country. On balance, however, the new sources of data and new tools available are proving to be a boon to government surveillance and law enforcement. We do not need to ignore traditional standards in order to respond to the new technologies. The attempt to literally translate all current surveillance capabilities directly onto the Internet may not be possible or desirable in all cases, or may require new privacy protections.

**Example 1 – Sample Web Packet (Chairman Hatch's Web Site)**[6]

```
Packet 3704
        Timestamp:                      13:38:40.765533
        Source Ethernet Address:        00:05:02:00:75:40
        Destination Ethernet Address:   00:D0:58:A9:30:52
        Encapsulated Protocol:          IP
IP Header
        Version:                        4
        Header Length:                      20 bytes
        Service Type:                   0x00
        Datagram Length:                384 bytes
        Identification:                 0x7D64
        Flags:                          MF=off, DF=on
        Fragment Offset:                0
        TTL:                            255
        Encapsulated Protocol:          TCP
        Header Checksum:                0x16B6
        Source IP Address:              207.226.3.15
        Destination IP Address:         199.95.76.12
TCP Header
        Source Port:                    1844 (<unknown>)
        Destination Port:               80 (http)
        Sequence Number:                0941715457
        Acknowledgement Number:         2963927064
        Header Length:                      20 bytes (data=344)
        Flags:                          URG=off, ACK=on,  PSH=on
                                        RST=off, SYN=off, FIN=off
        Window Advertisement:               17520 bytes
        Checksum:                       0xAC87
        Urgent Pointer:                 0
TCP Data
        GET /~hatch/greeting.ram HTTP/1.0.
        Referer: http://www.senate.gov/~hatch/.
        Connection: Keep-Alive.
        User-Agent: Mozilla/4.72 [Macintosh; U; PPC].
        Host: www.senate.gov.
        Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*.
        Accept-Encoding: gzip.
        Accept-Language: en.
        Accept-Charset: iso-8859-1,*,utf-8.
        Cookie: STATE=UT.
```

---

This data packet was collected from CDT's network while I was viewing Chairman Hatch's web site.

The header of the packet includes the source and destination IP addresses. In this case, the source IP address 207.226.3.15 is a computer at CDT and the destination 199.95.76.12 is the U.S. Senate web server. (If you type 199.95.76.12 into your browser after http://, it takes you to the Senate home page just as if you had typed www.senate.gov.) So the header, which can be easily separated from the content payload, would provide information similar to the

---

[6] The tools used in the packet collection for these three examples are freeware tools available for UNIX operating systems. The packet sniffing was done by tcpdump written by Van Jacobson, Craig Leres and Steven McCanne of the Lawrence Berkeley National Laboratory. The formatting of the packets into text was done by tcpshow written by Mike Ryan.

information that a pen register would provide on a person at CDT who called 224-3121, the Senate switchboard.

However, if the FBI wanted to know what precise page I was viewing, they would need to reach into the content ("TCP data") portion of the packet. There they would find that I had asked for ("GET"), a copy of /~hatch/greeting.ram. Anybody typing that into a browser would find that I had downloaded the video greeting on the Chairman's web page. Thus, they would know the precise content of my Web viewing.

**Example 2 – 3 Sample IP Packets – Email Message**

```
Packet 145
        Timestamp:                      13:16:01.877863
        Source Ethernet Address:        00:05:02:00:75:40
        Destination Ethernet Address:   00:D0:58:A9:30:52
        Encapsulated Protocol:          IP
IP Header
        Version:                        4
        Header Length:                        20 bytes
        Service Type:                   0x00
        Datagram Length:                80 bytes
        Identification:                 0x164E
        Flags:                          MF=off, DF=on
        Fragment Offset:                0
        TTL:                            255
        Encapsulated Protocol:          TCP
        Header Checksum:                0xB629
        Source IP Address:              207.226.3.15
        Destination IP Address:         205.252.14.66
TCP Header
        Source Port:                    2681 (<unknown>)
        Destination Port:               25 (smtp)
        Sequence Number:                0758931484
        Acknowledgement Number:         1689679905
        Header Length:                        20 bytes (data=40)
        Flags:                          URG=off, ACK=on,  PSH=on
                                        RST=off, SYN=off, FIN=off
        Window Advertisement:                 17520 bytes
        Checksum:                       0xE821
        Urgent Pointer:                 0
TCP Data
        MAIL FROM:<jdempsey@cdt.org> size=1024.
```

---

```
Packet 148
        Timestamp:                      13:16:01.997987
        Source Ethernet Address:        00:05:02:00:75:40
        Destination Ethernet Address:   00:D0:58:A9:30:52
        Encapsulated Protocol:          IP
IP Header
        Version:                        4
        Header Length:                        20 bytes
        Service Type:                   0x00
        Datagram Length:                87 bytes
        Identification:                 0x164F
        Flags:                          MF=off, DF=on
        Fragment Offset:                0
        TTL:                            255
        Encapsulated Protocol:          TCP
        Header Checksum:                0xB621
        Source IP Address:              207.226.3.15
        Destination IP Address:         205.252.14.66
TCP Header
        Source Port:                    2681 (<unknown>)
        Destination Port:               25 (smtp)
        Sequence Number:                0758931524
        Acknowledgement Number:         1689679948
        Header Length:                        20 bytes (data=47)
        Flags:                          URG=off, ACK=on,  PSH=on
                                        RST=off, SYN=off, FIN=off
        Window Advertisement:                 17520 bytes
        Checksum:                       0xDF9E
        Urgent Pointer:                 0
TCP Data
```

```
      RCPT TO:<makan_delrahim@judiciary.senate.gov>.
```

---

```
Packet 162
      Timestamp:                        13:16:02.417351
      Source Ethernet Address:          00:05:02:00:75:40
      Destination Ethernet Address:     00:D0:58:A9:30:52
      Encapsulated Protocol:            IP
IP Header
      Version:                          4
      Header Length:                          20 bytes
      Service Type:                     0x00
      Datagram Length:                  743 bytes
      Identification:                   0x1653
      Flags:                            MF=off, DF=on
      Fragment Offset:                  0
      TTL:                              255
      Encapsulated Protocol:            TCP
      Header Checksum:                  0xB38D
      Source IP Address:                207.226.3.15
      Destination IP Address:           205.252.14.66
TCP Header
      Source Port:                      2681 (<unknown>)
      Destination Port:                 25 (smtp)
      Sequence Number:                  0758931680
      Acknowledgement Number:           1689680063
      Header Length:                          20 bytes (data=703)
      Flags:                            URG=off, ACK=on,  PSH=on
                                        RST=off, SYN=off, FIN=off
      Window Advertisement:                   17520 bytes
      Checksum:                         0x7894
      Urgent Pointer:                   0
TCP Data
      Content-Type: text/plain; charset="us-ascii".
      Date: Thu, 31 Aug 2000 13:06:43 -0400.
      To: makan_delrahim@judiciary.senate.gov.
      From: Jim Dempsey <jdempsey@cdt.org>.
      Subject: Upcoming Carnivore hearing.

      Makan,
      .
      I might want to use some slides to illustrate some points in my testimony..
      Would it be possible to have an overhead projector available at the witness.
      table on Wed?.

      Thanks,.
      .
      Jim Dempsey.
      .
      Center for Democracy and Technology.
      1634 I Street, NW Suite 1100.
      Washington DC, 20006.
      voice: 202.637.9800       fax: 202.637.0968.
      jdempsey@cdt.org.
      .
      Use Operation Opt-Out http://opt-out.cdt.org/.
      A single place to remove your name.
      from profiling, marketing, and research databases..
      .
      .
```

---

These three data packets were collected from CDT's network when a computer on the network sent an email message from Jim Dempsey to Makan Delrahim, a member of the Committee staff. To send the entire email message required about 20 packets, although the

text of the message actually fit within one packet. All the other packets were involved in setting up the communication.

Each packet has a two part header that includes the source and destination IP addresses. In this case the source 207.226.3.43 is a computer at CDT and the destination 205.252.14.66 is our ISP's mail server (which will receive the packet and send it to the Senate mail server based on its content.) It would be trivial for an ISP to isolate packets to and from these IP addresses and to strip off the headers and provide only them to the government.

But if the FBI wanted to use the packets above to determine the "To:" and "From:" lines under a pen register order, as it claims it has the authority to do, it wold not find that in the headers. It would have to analyze the "payload" or contents of the packets in order to retrieve the address of the email sender and recipient. In the example above, the "From:" information comprises the entire content payload of packet 145, and the "To:" information comprises the entire content payload of packet 148. If Carnivore were able to record just these two packets, it would be collecting only the addressing information. But if Carnivore recorded all packets from the IP address 207.226.3.43, it would be recording the content of the message, since packet 162 contains the full text of the message itself.

**Example 3 – Sample Web Packet (Barnes & Noble.com Web Site)**

```
1 TIME:   15:02:27.439225 (0.111930)
2 LINK:   00:80:19:42:21:68 -> 00:D0:58:A9:30:52 type=IP
3   IP:   207.226.3.43 -> 208.158.245.141 hlen=20 TOS=00 dgramlen=695 id=6638
4         MF/DF=0/1 frag=0 TTL=255 proto=TCP cksum=79CE
5  TCP:   port 1559 -> http seq=3306680833 ack=0184661700
6         hlen=20 (data=655) UAPRSF=011000 wnd=17520 cksum=C1DE urg=0
7 DATA:   GET /booksearch/results.asp?WRD=prostate+cancer&userid=4MOT3
8         F70ED HTTP/1.0.
9         Referer: http://www.bn.com/.
10        Connection: Keep-Alive.
11        User-Agent: Mozilla/4.72 (Macintosh; U; PPC).
12        Host: shop.barnesandnoble.com.
13        Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
14         image/png, */*.
15        Accept-Encoding: gzip.
16        Accept-Language: en.
17        Accept-Charset: iso-8859-1,*,utf-8.
18        Cookie: SITESERVER=ID=3b671bc4c04048950bc8a20a61c31d96; brow
19        serid=BITS=0&OS=4&VERSION=4%2E72&AOLVER=0&BROWSER=1; Shopper
20        Manager%2FBNShop=SHOPPERMANAGER%2FBNSHOP=2D9DNPCEB6S92MJ1001
21        PQUW93SAR9582; userid=2NW5T2ANM7; SalesURL=Rwww%2Ebn%2Ecom%2
22        F; ASPSESSIONIDQGQGQQCD=NACHKFKCMBPBEANEEODHLDAI.
```

---

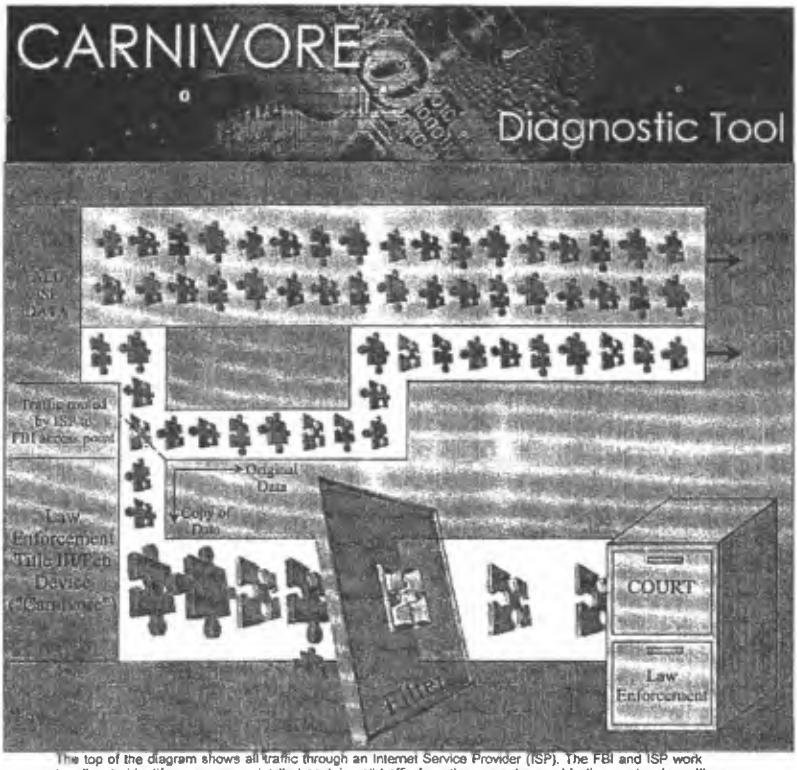
This data packet was collected from CDT's network when someone at CDT was searching for a book on the Barnes & Noble web site relating to "prostate cancer."

The header of the packet includes the source and destination IP addresses (line 3). In this case, the source 207.226.3.43 is a computer at CDT and the destination 208.158.245.141 is a web server affiliated with Barnes & Noble.com.

The information about the specific web page that the CDT computer viewed is contained in the packet's data section, starting at line 7. The URL shown here:

> http://shop.barnesandnoble.com/booksearch/results.asp?WRD=prostate+cancer&userid=4MOT3F70ED

tells what books are being viewed – in this case, books about prostate cancer, just as if one had intercepted a telephone call to Barnes and Noble asking if it had any books in stock about prostrate cancer. The content section of subsequent packets would show which of these books was purchased.




The top of the diagram shows all traffic through an Internet Service Provider (ISP). The FBI and ISP work together to identify an access point that contains all traffic from the suspect named in the court order, with as little other traffic as possible. In some cases, the ISP is able to provide the FBI with an access point that contains only the suspect's traffic.

The FBI connects a commercially available one-way tapping device at the ISP's access point. This tap produces an exact copy of all data at the access point. The tap also provides electrical isolation to prevent Carnivore from having any kind of impact on the ISP's network.

The copied network traffic then flows into the collection system where it is compared against a predefined filter. This filter only passes traffic authorized for capture by the court order. Traffic that passes through the filter continues on to be archived to permanent storage media. No other data is ever stored to permanent media, nor is any information recorded about traffic that does not match the filters.

All information collected is maintained and, in the case of full content interceptions, is sealed under the order of the court. This information, as well as information obtained pursuant to pen register and trap & trace authorities may subsequently be made available by the court to the defendant.

---

| Carnivore | Carnivore Home | Programs & Initiatives | FBI Home |

The CHAIRMAN. Professor Rosen, we will conclude with you. We would like to have some questions here before we finish.

**STATEMENT OF JEFFREY ROSEN**

Mr. ROSEN. Thank you so much, Senator. It is an honor to be here. I just want to talk very briefly at the end of this hearing about uncertainty, and in particular about the cost of the uncertainty that results from covert monitoring on the Internet, and this is the uncertainty of innocent citizens who can't be sure whether or not their intimate communications are being intercepted by State officials or by ISP's.

It strikes me that even at the end of this fascinating and informative hearing, there is a great deal of uncertainty that continues to be associated with Carnivore. I was interested and encouraged to hear Dr. Kerr testify that Carnivore is only made available to ISP's if they are unwilling or unable to conduct the search themselves, and that it is removed as soon as the court order expires. Surely, this procedural regulation should be codified to reduce the uncertainty of innocent citizens who may fear that their Government has technical access to their messages without their knowledge or consent.

There are, as you began by saying, Senator Hatch, other uncertainties associated with Carnivore. The FBI is legally forbidden from monitoring the communications of citizens who are not targets, but the mere knowledge that Government agents have the technical capacity to read e-mail messages will greatly increase the uncertainty of innocent citizens at a time of widespread concern over privacy over the Internet.

It is also true that one of the safeguards of the system, the audit trail records that record precisely which communications are intercepted, is made available to targets only if a prosecution actually results. So innocent citizens who are not targets have no notice when they are being monitored and no confidence that they are not being monitored.

Senator Hatch, I would be delighted to give you a copy of my book. It is called "The Unwanted Gaze: The Destruction of Privacy in America," available everywhere from Random House. And I will take this opportunity to note that the title, "The Unwanted Gaze," actually describes the consequences when people are not certain about whether or not they are being observed.

It comes from a beautiful passage actually in Jewish law that describes the anxiety and inhibition that results when citizens are being watched without their knowledge. There is a body of doctrine called hezzek re'iyyah, which means the injury caused by seeing or the injury caused by being seen. So when your neighbor puts up a window, observing you in a common courtyard, you are entitled not only to prohibit the neighbor from observing you, but also actually to require that the window be taken down because medieval authorities recognized that it was not only the surveillance itself, but uncertainty about whether or not surveillance is taking place, that forces us to lead more constricted lives and inhibits us from speaking and acting freely in private places.

So, understandably, the consensus among these medieval jurists was that the window had to come down even if the individual

whose privacy was violated failed to protest because there was this uncertainty that made everyone act in a more inhibited way in spaces that should be considered private.

I am concerned particularly at this moment of uncertainty about the Internet that the Carnivore System, even if it were administered scrupulously, would increase the anxiety about monitoring on the Internet at precisely the moment when many citizens are afraid to use e-mail because of concerns about privacy.

There are several surveys of the health effects of monitoring in the workplace that suggest that electronically-monitored workers express higher levels of depression, tension and anxiety, and lower levels of productivity than those who are not monitored.

Now, let me briefly address the constitutional issue which has been touched on, but seems to me a very hard one, and this is the question does Carnivore violate the fourth amendment. It seems to me that one could make a strong argument on either side. Is this the quintessential example of an unreasonable search or is it the precisely tailored example of the perfectly reasonable search?

Carnivore operates very much like an ingenious and hypothetical search that was discussed in a fascinating article in the Yale Law Journal recently, and this is a program called the worm. So the worm is a form of computer software that the Government can dispatch to enter your computer without notice. It scans your hard drive for illegal software or specified words or images, pornographic pictures or any other evidence that the Government is looking for. If the worm finds what it is looking for, it can alert the FBI. And if not, it destroys itself, leaving no trace of its presence.

So in some respects, the worm seems very much like Carnivore, and it looks precisely like the general warrants that the Framers of the fourth amendment meant to prohibit. Both Carnivore and the worm can monitor millions of computer users without probable cause to believe that a crime has been committed, and they search broadly without particularized suspicion of people or places.

But in other respects, the worm, like Carnivore, avoids all of the spillover effects that led the Framers of the fourth amendment to condemn general warrants in the first place. Rather than exposing innocent as well as illegal material, it focuses on the illegal material with greater precision.

So, Senator Leahy, you began by noting that in the 18th century if you wanted to read someone's diary, you had to break into their house and rifle through their desk drawer, and then you would see a lot of innocent information in the course of searching for guilty information. Carnivore, if properly administered, might be said to avoid all of those effects and only reveal the guilty information. So I don't think we should be alarmist or hyperbolic about this difficult question of constitutional translation.

Senator LEAHY. Are there people who are being alarmist or hyperbolic here?

Mr. ROSEN. Are people being hyperbolic? I should say that I have a hyperbolic instinct when I hear about Carnivore because my fourth amendment knee jerks. But when we think about this responsibly, it seems to me a hard constitutional question.

Senator, let's remind ourselves, too, how far we have moved from the world of searches of private diaries in desk drawers. In the

18th century, the search of a private diary was considered the quintessential example of an unreasonable search. We have the story of John Wilkes, the famous English patriot whose diary was searched by King George, sued in trespass and won ruinous damages. It is only recently that private diaries have lost their constitutional protection, we learned from the case of Senator Packwood.

It is also true that in the famous article about the right to privacy written by the future Justice Brandeis, he noted that if a man wrote in a letter to his wife that he hadn't dined with his son that day, not only the content of the letter but also a general list of its subject matter would be protected from public exposure because it wasn't the information itself, but the domestic occurrence.

We have fallen very far from there to a world where the list of the subject matters of e-mails are available on a general standard of relevancy. And one of the things you might consider, Senator, because I know both of you have been so important in thinking about pen registers, is whether a higher standard for the subject matter of e-mails, some more like reasonable cause, might be appropriate.

I will conclude by echoing Michael O'Neill's notion that the search of this subject matter information seems far more invasive than a pen register because they reveal so much more identity, both the names of the recipient and the sender, and in the case of URL's the bookstores that you have searched and the actual search terms themselves. So this is why a reasonable cause standard might be appropriate.

It seems to me that none of the FBI's testimony at previous hearings suggests compelling reasons why e-mail interception should depart from traditional statutory models for regulating wiretaps. I agree with James Dempsey that Internet service providers rather than the FBI should at least have the first opportunity of producing relevant communications specified by a court order, and Carnivore should not be imposed but made available to those who can't afford to undertake this search.

You might also think about other possibilities, keeping audit logs for all communications monitored by Carnivore, not simply those that result in prosecution, and increasing procedural protections for innocent communications to reduce the uncertainty of citizens who have no notice about whether or not monitoring has occurred.

But my big point is just the costs of uncertainty are great. This is an anxious time for the Internet. At the very least, innocent citizens need to be reassured that their Government is not observing their intimate messages without their knowledge or consent.

Thank you.

The CHAIRMAN. Mr. Cerf, let me just turn to you first, and perhaps I should express the gratitude of the Vice President for your assistance in helping him to invent the Internet. [Laughter.]

I just couldn't resist.

I notice you had some differences, or at least you looked like you had some differences with Professor Rosen. I will give you a chance to respond.

Mr. CERF. Senator, I am sorry. I am having trouble hearing you. I am hearing-impaired and my hearing aids are not picking you up.

The CHAIRMAN. That is fine. I do have a soft voice, too soft—my wife says.

I noticed you had some difficulties with what Professor Rosen was saying.

Mr. CERF. I had some reactions.

The CHAIRMAN. I would like to see what you have to say.

Mr. CERF. I would like to suggest two things to our panelists. One suggestion about putting the Carnivore software, or the equivalent thereof, in the hands of the ISPs for purposes of having them perform these searches strikes me as alarming, frankly.

If I were a member of the public wondering who is managing that software and doing things with it, I would be more concerned if it were available to and generally in use by ISP personnel, who need not necessarily understand or follow all the restrictions and constraints that the FBI would follow. So it seems to proliferate that strikes me as being excessive compared to what the FBI proposes, as I understand it, which is to place the equipment there only during the period of time that surveillance is required and then remove it again.

Have I misunderstood that?

Mr. KERR. No. That is correct.

Mr. CERF. So in some sense, the proposition puts the facility at broader spread than it would otherwise. That is one point.

You wanted to respond to that?

Mr. DEMPSEY. Well, I was just going to say that this use of Carnivore or unauthorized access to electronic communications is equally a crime. The sanctions are the same and the definition of the offense is the same——

Mr. CERF. No debate there.

Mr. DEMPSEY [continuing]. Whether it is done by Government officials or by ISP's.

Mr. CERF. But I have the feeling that the ISP geeks may be less familiar with the penalties and with the restraints than the gentlemen from the FBI. So I would propose that that is not the best idea in the whole world.

The other reaction that I had, Mr. Chairman, was any comparison of the Carnivore system with the worm is technically ill considered. The worm is a very different kind of beast. It is a mobile piece of software. That is not the way the Carnivore system functions.

I did have the opportunity to go down to Quantico and have a pretty thorough briefing and to see the Carnivore system in operation. I regret that other members of the technical community appear to have felt unable to do that or are reluctant to do so. It was a helpful briefing, and I feel as though I have a much more firm understanding of what it can and cannot do.

I still have concerns about it, as you could tell, I hope, from my comments on how much you have to look at in order to filter appropriate content. But I think the comparison with the worm is not well considered and I think should be rethought, Mr. Rosen.

Mr. ROSEN. I should suggest I was not making a technical comparison between Carnivore and the worm, but simply in the nature of the focused search. Limited to that particular aspect, it seems to me they are exactly analogous in the sense that it only reveals

the information it is looking for and doesn't reveal to any human agent information it is not looking for. That was the limit of the comparison.

Mr. CERF. OK, then you are not proposing that the Carnivore is a mobile piece of software that moves around and jumps into millions of machines, which it does not do?

Mr. ROSEN. I am a lawyer, not a technician, sir. I will defer to you on——

Mr. CERF. I will forgive you for that.

Mr. O'Neill. If I could just make a point, sort of a means of follow-up, I think one of the difficulties and what perhaps concerns people is the idea that there is software and also hardware, because Carnivore apparently is both, and it is unclear precisely what it does or what its capabilities either currently are or can be.

I mean, we all know—and I am not a technician particularly either, but we all know that software is not only dependent upon what it is, but how it is updatable, how it is modifiable, and how in any individual case it can be configured.

Now, I happen to be not in the camp of those who would like to see the Carnivore source code released to the public. I think that would, in part, defeat its purpose. But I do think that it is important for this body to have oversight to make sure that at least someone is watching the watchers. And it seems to me that that is the important role that Congress can play in this whole decision-making process.

The CHAIRMAN. Go ahead.

Mr. CERF. Well, I am thinking that the existing surveillance mechanisms are in place now and we must have someone watching the watchers, I hope. I mean, I would assume that that is true. So wouldn't the same watchers who currently oversee this——

Senator LEAHY. Don't always assume that, Mr. Cerf.

The CHAIRMAN. No, you can't always assume that.

Mr. CERF. I am sorry?

Senator LEAHY. I said don't always assume that.

Mr. CERF. Well, all right. If I am incorrect, then we have a bigger problem than just Carnivore.

The CHAIRMAN. It is a big problem. We want you to know it is a big problem.

Professor O'Neill, you gave us 10 reasons that you didn't define, but let me just go through those. No. 1, you say with respect to Carnivore itself, Congress ought to obtain briefings, classified if necessary, to get a better understanding of what Carnivore is designed to do, how it does it, and whether there exists potential for abuse.

No. 2, Congress ought to determine what the statutory authorization for Carnivore is and whether law enforcement has the authority to insist that a service provider install Carnivore.

No. 3, if implemented in some fashion, Congress should require that statistics be maintained by the Justice Department and that these so-called, "audit trails," be routinely provided for legislative oversight.

No. 4, Congress should seek to learn whether Carnivore can easily be defeated by encryption software or E.A. Poe-type purloined letter schemes.

More broadly, No. 5, hearings ought to be conducted to determine whether all Internet trap and trace orders should be issued only on the basis of the judicial finding that reasonable cause exists to believe that a target has or is about to commit a crime.

No. 6, the executive branch ought to be required to provide consumers with notice whenever the Government obtains information about their Internet transactions.

No. 7, specific statistical reports for pen register or trap orders for Internet communications similar to the reports required under title III ought to be required.

No. 8, Congress should explicitly provide that Internet queries, e-mail subject lines, URL's of sites visited, and other information which provides more than the equivalent of a dialed number cannot be disclosed without a probable cause order.

No. 9, Congress should consider requiring notice and opportunity for defendants to object when civil subpoenas seek personal information about Internet usage.

And, No. 10, provide enhance protection for information on networks, probable cause for seizure without prior notice, and a meaningful opportunity to object for subpoena access.

Then you say, "At bottom, I would urge a cautious, thoughtful approach when it comes to expanding surveillance capabilities. The conflict between increased security and enhanced privacy protection is not easily resolvable, nor will it likely ever be. But Congress ought to seize the moment to ensure that robust debate occurs before law enforcement's powers are enhanced and regardless of how the balance is struck."

I thought those were pretty good suggestions, to be honest with you. I don't know how the FBI feels, but having heard them, what do you think, Mr. Kerr.

Mr. KERR. Well, I must say that I have just heard them for the first time, as you have read them off.

But if you would permit me, Mr. Chairman, there were some questions and suggestions raised about our interactions with the Internet service providers and I think I can help you on that.

The CHAIRMAN. Well, let me add to that because it was raised here in this article in USA Today, which I have read—it appears to cast doubt on whether any university is willing to take the study of Carnivore under the restrictions that have been placed on such a study by the FBI, or at least the restrictions they think are placed by the FBI. In fact, Mr. Dempsey has pointed that out, I think, fairly strongly, and I would just like you to comment about that in your overall comments.

Mr. KERR. All right. The first point I should make absolutely clear is that the FBI is not soliciting this review. It is being done by the Department of Justice, and in particular under the auspices of Steve Colgate, the Assistant Attorney General, head of the Justice Management Division.

While I will be part of reviewing the report once it is prepared, I will have nothing to do with determining the scope of that study or the acceptability of the outcome. We did it precisely to avoid having the FBI funding a look at its own equipment and capabilities.

Senator LEAHY. Does the FBI support the study, though?

Mr. KERR. Yes, absolutely.

Senator LEAHY. Thank you.

The CHAIRMAN. Have you set the restrictions on the study, though, or has the Justice Department set the restrictions?

Mr. KERR. The Justice Department.

The CHAIRMAN. Mr. Di Gregory, is that right?

Mr. DI GREGORY. That is correct, Senator.

The CHAIRMAN. Why have restrictions?

Mr. DI GREGORY. Well, there are certain restrictions that we believe are necessary. The one restriction, for example, is the restriction on the release of the source code. We don't believe that the source code should be released publicly because that could hamper law enforcement efforts.

The CHAIRMAN. I can understand that.

Mr. DI GREGORY. And a general restriction with respect to the scope and the nature of the review is that the review is a technical review. The review was never intended to be a legal review, but a technical review to determine whether or not Carnivore does the things it claims it does.

The CHAIRMAN. Then why are these universities having such a difficult time taking on that review?

Mr. DI GREGORY. I don't know. That is probably a question you would have to ask the particular universities involved, and I can't comment any further on the procurement process.

The CHAIRMAN. But am I correct in inferring that all the universities approached thus far have refused to take on the review?

Mr. DI GREGORY. First of all, I don't know the answer to that, and even if I did know, I wouldn't comment on it because there are restrictions with respect to commenting on the procurement process that I am not completely familiar with, but am familiar enough with to know that I don't want to get in trouble. So if you wouldn't mind my——

The CHAIRMAN. Well, you don't want to get in trouble with us either, do you?

Mr. DI GREGORY. I don't, Senator. [Laughter.]

The CHAIRMAN. I understand.

Mr. O'NEILL. One thing I would add to that, Senator, is it is interesting, though, that—and I think the Department of Justice ought to be commended for taking these steps, but I think it is interesting that it seems to be—if you sort of follow the time line, at least, it is in large part because Congress chose to take oversight of this because this information was leaked to the press that the Department of Justice then sought this outside independent review, which is entirely the appropriate and proper thing to do, and it is, of course, the role that Congress ought to be playing here.

The CHAIRMAN. Well, your ten suggestions are very broadly written. I would like you and Mr. Rosen and others, and especially you, Mr. Cerf and Mr. Dempsey, to look at these and see if you can improve upon them and make suggestions for us and for the Justice Department and for the FBI as to how we might do this.

Look, this is something that is really terrifying a lot of people around the country. Are we going to have an Orwellian type of investigative Government now that we are in this Orwellian type of a world which is doubling now in capacities in revolutionary ways?

This is scary stuff. We have people who don't want anything to be done in this area. And, of course, we have people that are terrified that if we keep allowing the Internet to be used as a source for crime and criminal activity, this society is going to be very badly damaged. So I would like you all to spend some time on that.

Mr. Cerf, go ahead, and then I will go to Mr. Kerr.

Mr. CERF. There is a book that was published recently by a gentleman named Amitai Etzione. The title, if I remember correctly, is something like "The Limits to Privacy."

The CHAIRMAN. Right.

Mr. CERF. In that book is what I thought was a fairly reasoned and balanced discourse about the protection of personal privacy.

The CHAIRMAN. And you think Etzione's discourse would apply in this case, in this digital world?

Mr. CERF. You say it would not apply?

The CHAIRMAN. No. Do you think it would apply?

Mr. CERF. I believe that it would because his premise is that there is a balance to be reached, as I think several panelists have said, between the protection of personal privacy and personal information, and the need to protect the general public's well-being from people who don't mean it well, criminal elements.

And what Etzione argues in this book is that it is possible that we have gone too far in one direction or another. It is a worthwhile book to read, if only to be provoked into thinking about what the balance could be or should be.

The CHAIRMAN. Mr. Kerr.

Mr. KERR. Two points that I would like to make very briefly, Mr. Chairman. First, the suggestion that in any way information about Carnivore was leaked to the press and has led to hearings and press coverage is absolutely wrong. We have been briefing on Carnivore for about 18 months. It has been reviewed substantially within the Department of Justice. It has been briefed to many companies, many trade associations.

We have offered two ISP's complete access for them to review the product and its performance, and in no way have we attempted to conceal its existence or its intended purpose. And so I find it rather surprising at this juncture that that is still the view. We have briefed many members of the congressional staff as well.

With respect to the concern about ISP's and their access, the thing we safeguard is the integrity of the evidence. The box where we record the information is locked and accessible only to an FBI agent. Also, the PC on which the system is based has its keyboard and monitor removed so that, in fact, a passer-by can't make a change either maliciously or inadvertently. And we don't allow them to use the remote dial-up access which we employ and log, but that is what tells us when the memory is full and an agent needs to go and remove the disk.

So we have tried to design it not only with great specificity to respond to the court orders, but, in fact, with a view toward maintaining the integrity and authenticity of the evidence we collect, and to be able to testify after the fact in court that we did so, who had access, when they had access, and what the settings of the device were.

I hope that clarifies the point.

The CHAIRMAN. Well, it helps, except for one thing. As I understand your testimony, you indicated that Carnivore has been used in some 25 cases so far. Is that correct?

Mr. KERR. Yes, sir. It is now between 25 and 30. That is correct.

The CHAIRMAN. There are reports that the Attorney General was not aware of it—according to press reports, was not aware of Carnivore. And I hear from constituents that their concern with Government surveillance is not their objection to authorized uses of it, but the potential uses without the proper checks and balances on Government search and seizure that our country and Constitution are based on.

What concerns most citizens and concerns me deeply are reports that the FBI developed and deployed the Carnivore system without even the knowledge of the Attorney General herself. That may be par for the course for this Justice Department, but you cannot take this lightly, given the fundamental civil liberties that are implicated here.

Now, my sense is that much of the controversy surrounding Carnivore is due to the apparent perception, rightly or wrongly—and I would like you to clarify this—that there is no check on its use by the FBI. Now, I would like, Mr. Kerr, you and Mr. Di Gregory to explain to us to what extent the development and deployment of new surveillance technologies by Federal law enforcement have to be authorized by Congress.

In other words, under what delegated authorities are new technologies, in general—and Carnivore in particular—developed, and was there specific authorization by Congress or the Attorney General to develop and use Carnivore or other similar systems?

Are these press reports right that the Attorney General didn't even know about it until recently? And answer the question as far as what rights do you have to go ahead with it.

Mr. KERR. Mr. Di Gregory is going to give the first part of the answer and I will give the second.

The CHAIRMAN. Okay, that will be great.

Mr. DI GREGORY. From what I understand, Senator, without knowing of the name "Carnivore" or without knowing of the specific program—this is my understanding—the Attorney General was aware of the FBI's capacity to do this kind of surveillance. I think Ms. Stansell-Gamm may have some more detail about that.

The CHAIRMAN. But the Attorney General was unaware of the actual software that was being developed or has been developed?

Ms. STANSELL-GAMM. I simply don't know at what point the Attorney General became aware of this specific tool or the name of the tool.

The CHAIRMAN. Then answer the second question. What authority do you have to do this and to have used it in 25 cases? Has Congress given you any authority?

Mr. KERR. Well, in fact, Congress appropriated the money, pursuant to our budget request, within which there is a specific line related to electronic surveillance, and particularly the development of tools for access to data networks, the Internet, and the like. It has been in our budget for a number of years. It is part of our continuing response to be able to carry out our mission to lawfully intercept communications as technology evolves.

The CHAIRMAN. We are happy to have Mr. Parkinson and Ms. Stansell-Gamm here with us today.

Ms. STANSELL-GAMM. I would like to answer your question another way, if I could. It has been at least 3 years ago since the Attorney General made a press announcement about the case called Ardita, which Mr. Dempsey referred to, kindly, as one of our law enforcement success stories. And she briefed that case in great detail to the press, and the core of that story was what we were able to do and how we were able to do it.

It involved an electronic wiretap at a network at Harvard University that this hacker, who turned out to be in Argentina, was using as a platform for attacking DOD systems all over the world. The investigative problem that we had was how to find the needle in the haystack, how to find Mr. Ardita's communications in the haystack of legitimate traffic.

The Attorney General understood how we were able to do that, which was supervised very closely by a court in Boston. I think there were two separate title III orders. And because the tool that we were using to do that was a tool that was not as sophisticated as Carnivore but, as Mr. Cerf has pointed out, captured a great deal more hay than the needle, the minimizing process was far more exacting, required several steps and, in fact, required an agent to look at some text strings.

The irony of all of this is that while——

Senator LEAHY. Instead of carnivore, was that omnivore?

Mr. STANSELL-GAMM. No, that was not omnivore. In fact, it was a tool developed by the Navy called NIDS, Network Intrusion Defense System. The Air Force has one that they call Sniffy. You know, they all have their different names, but these tools have been used by law enforcement in a variety of agencies for some time, under the strict supervision of courts.

As I say, the irony of all of this is that the tool Carnivore is the most selective, the most discreet, the most controllable, the one that is most likely to be able to reach in and pull out only the needle, although, as you say, it is a very hard problem.

The CHAIRMAN. Maybe bits of needles.

Ms. STANSELL-GAMM. Bits of needles, exactly, while the haystack is moving by.

The CHAIRMAN. Right.

Ms. STANSELL-GAMM. It is a very difficult technological challenge. So this represents, in my view, quite a good-faith attempt on the part of the FBI engineers to respond to the challenge of collecting information on the Internet in ways that comply strictly with our legal authorities, and to do it in very discreet, controlled ways that create records. That is what this tool does.

The CHAIRMAN. Let me turn to Senator Leahy. I have taken long enough.

Senator LEAHY. You know, it is interesting as we examine these issues to look back at lost opportunities. A few years ago, I suggested some better procedures for applying for warrants on pen registers, and so forth, and the FBI has always been reluctant to talk about that.

Now, I find, since Carnivore came out, some of my colleagues in the House have proposed that we change not just the procedures,

but also the standard for pen registers and traps and traces to an extent that I think that probably Justice and the FBI would wish that they had paid more attention to the suggestions that I made. But I assume from the fact that they haven't expressed any change of heart about my prior proposal that, they reject that and would prefer that I support the legislation, for example, of Representatives Canady and Hutchinson, H.R. 5018, which proposes a more stringent standard for pen registers, trap and trace, and similar devices that would identify e-mail addresses, like Carnivore.

That legislation would require specific and articulable facts reasonably indicating that a crime has been or is being or will be committed, plus a showing of relevance of the information sought to the investigation of that crime. Another bill introduced by Representatives Barr and Emerson, H.R. 4987, would apply that same greater standard to all pen registers and traps and traces, whether or not they would identify e-mail addresses.

Since the source and destination information about e-mail may have content in a way that a dialed telephone does not, should we change the standard for pen registers and traps and traces, or do my earlier suggestions now suddenly sound better to you?

Mr. DI GREGORY. As you may know, Senator, the administration has put forth a proposal which would elevate the standard required for trap and trace or pen register information, though not quite the same standard that is put forth by Barr and Canady. Our standard would require the prosecutor—the one that is proposed would require the prosecutor to submit a factual statement rather than merely a certification, and that that factual statement would be viewed by a court and a court would determine whether or not the factual statement was sufficient to establish that the information to be obtained from pen register or trap and trace was information relevant to an ongoing criminal investigation.

Senator LEAHY. Does that mean you don't like their legislation?

Mr. DI GREGORY. There are problems with their legislation. The one that comes to mind initially is that the legislation submitted by specifically Representative Canady is e-mail-specific. It is not even Internet-specific, but it is e-mail-specific, and that creates a problem.

As we have said in other contexts and have said before Chairman Canady's subcommittee, we believe that any legislation that is developed with respect to the substantive criminal law, or even the procedural criminal law as it relates to the Internet should be as much as possible technology-neutral. We don't think that there should be a different standard for the interception of e-mails versus the interception of telephones—excuse me; I used the word "interception"—for a pen register or a trap and trace for e-mails as opposed to a pen register or trap and trace for telephones.

Senator LEAHY. Dr. Kerr, do you feel the same way?

Mr. KERR. I will take the easy-out, sir. As you know, I am a physicist and I don't normally opine on matters of the law.

Senator LEAHY. Thank you. There is nothing wrong with that answer.

We got a letter from the FBI last month that described the operation of Carnivore. It said, "It does not snoop through e-mail trav-

eling through an ISP network by searching for key words or reading the subject line or any other content."

But the nature of how the Internet works, as I see it anyway, is that the specific communications or addressing information of a suspected criminal, one who has been targeted under a court order, are mixed all up like a stew with all the other packets of different Internet users carried by the ISP.

Somehow, Carnivore has to snoop through all these other different packets to find the right one, the needle in the haystack. Is that correct?

Mr. KERR. Let me start to answer and certainly welcome any assistance Mr. Cerf would like to give, but go back to his envelopes for a minute. What we are looking at in the first instance is the address on the outside of the envelope. With the address matching the one we are authorized to capture, we collect the envelope and we subsequently go and we only take from that envelope the information we are authorized to take.

But we use the addressing properties of the Internet itself, the Internet protocols, to select out just those packets. We don't read them at that point. The machine is doing it. There is no content being viewed by any human. And, in fact, those packets that contain information we are not authorized to obtain disappear at that point. We don't control them.

Senator LEAHY. But to use the envelope thing, it is like getting a big bag of envelopes and you are looking just for the one addressed to Dr. Kerr, but there is also an envelope in there to Mr. Parkinson, Mr. Di Gregory, and on and on. I mean, you have got to go down through all those envelopes at some point.

Mr. KERR. Well, think of it better perhaps, you are standing at the post office and all the envelopes are going by you on a conveyor belt. And we are just picking off those envelopes that have the right address on them. The others go away; they are not in our life anymore.

Senator LEAHY. Mr. Cerf.

Mr. CERF. If I could interject, the problem here is a language and terminology problem. The term "address" unfortunately is overused for a variety of different purposes even in the Internet. And so we speak, for example, of Internet addresses, by which we sometimes mean 170.127.34.16, which is a numeric indicator of where a computer is in the Internet. It is sort of like a telephone number.

On the other hand, we also say what is your Internet address, and by this we often mean what is your e-mail address, which in my case would be vcerf@mci.net. Those are different, and so the way the Carnivore works is it starts with the lowest-level physical numeric addresses of the source and destinations that are under observation. And it only selects out—the conveyer belt model is a good one—it only selects out those ones that happen to contain those physical addresses.

Now, we can argue separately about whether you have got the right addresses. I mean, there are some issues about the stability of IP address assignment and whether or not a particular computer has the same IP address forever and ever or whether it changes from time to time. I am sure that the members of this committee

don't want to know all the details right here on the spot, though I am prepared to provide them if needed.

But after you have selected the set of envelopes that may contain information of interest, only then do you then look inside. And if I have any concerns at all—and I want the FBI folks here to know I do have concerns—you do have to see quite a bit; you have to suck into the Carnivore machine quite a bit before you can find that part which you are interested in after you have determined that this envelope might contain something of interest.

The point that the Carnivore programmers make is that the software is intended to look at the collection of material that makes up an e-mail message like this one, that amount of which happens to be in one packet, and only if it finds, for example, a "to" and "from" e-mail does it capture that packet. If it can't find that, if it can't parse the contents, it throws it away. That is the design, that is the intent, and that is the way it is used. So it is true that the machine pulls in more than is needed, but it then is programmed to throw away that part which doesn't match their search criteria.

Senator LEAHY. And what you are saying, Dr. Kerr, is you can't go back to the machine and find out what was thrown away?

Mr. KERR. That is correct.

Mr. CERF. Except in the case, of course, where you have been authorized to obtain and capture content as well. I don't know whether you are ever allowed to do that.

Mr. KERR. The answer I was giving was that packets that we have discarded aren't available to us at all.

Mr. CERF. They are not. They have disappeared on the conveyor belt and have gone away. So it is a multilevel filter that is being applied, and at each stage in the filtering process less and less information is retained.

Senator LEAHY. Mr. Dempsey, you wanted to add something to that.

Mr. DEMPSEY. Yes, Senator. I have two comments, one of which addresses the question which is, is it good enough that Vint Cerf has looked at Carnivore and has come away relatively satisfied with it. And I have to say that——

Mr. CERF. I won't take any offense if you say that it isn't because I would agree with you.

Mr. DEMPSEY. That it isn't good enough?

Mr. CERF. That is right.

Mr. DEMPSEY. And so we have to somehow get beyond the fact that one person has been in, or that several people have been in. I really don't think we have had the kind of review of Carnivore that would really satisfy this committee and satisfy the public, and I do agree with the chairman that somehow the FBI needs to work and the Justice Department needs to work on that independent review.

I would note in response to Dr. Kerr's comments it is a Justice Department review, but this nondisclosure agreement which Vint Cerf signed but which other people are rather reluctant to sign—the nondisclosure agreement is between the contract personnel and the FBI. You are signing an agreement with the FBI and you are responsible to the FBI as to what you can say and not say.

I also think that I am a little bit reminded of the——

Senator LEAHY. Responsible to the FBI, even though the review is that of the Justice Department, or did I miss the point?

Mr. DEMPSEY. Well, the question was who is controlling the——

Senator LEAHY. You are talking about when it goes in.

Mr. DEMPSEY. Controlling the review.

Senator LEAHY. Yes, OK.

Mr. DEMPSEY. Who is controlling the review, and Dr. Kerr made the point, well, people needn't worry; it is a Justice Department-controlled review. And I am making the point that the nondisclosure—people are going to be bound to the FBI.

Mr. CERF. May I just interject that I agreed to sign the nondisclosure on the principle that when you are dealing with surveillance, just as you would with other intelligence situations, sources and methods are always a sensitive issue.

Mr. DEMPSEY. But the concern on the part of people, as I understand it, is that this agreement is so broadly drafted that it will prohibit people from talking more broadly or more generally. Now, you feel comfortable coming here today and speaking, but other people are worried, particularly if they would be critical as opposed to moderately supportive, that they would then be accused that they had—particularly if they talk about ways in which Carnivore may be vulnerable, may be subject to abuse, may be avoidable or evadable, that they would—the point is we need to get beyond one person knowing.

Mr. CERF. Absolutely, and I believe that the FBI has, in fact, introduced this system to more than one person.

But I just want to emphasize two things. First of all, I am conscious of the concern over methods of collection and I recognize the need to keep those reasonably under control. However, I do agree with Mr. Dempsey that one person is not enough and that you need a broader substantiation that this system does what it, in fact, claims to do. So I would certainly agree with what I think Mr. Dempsey is suggesting, is that there be a broader review of this system and some confirmation coming back to this committee that it does as it is advertised.

Senator LEAHY. I would like that.

And let me ask you—I think this would probably be for the FBI or DOJ—the D.C. Circuit Court of Appeals had a recent decision on the FCC's implementation of CALEA and it raised some interesting questions both about the legality of Carnivore, but also I think the liability of ISP's. The court agreed with the FCC that a standard adopted by telecommunications carriers could provide both packet headers and the content or payload to law enforcement.

The carriers argued, though, that they couldn't technically separate the two, while the FBI said, that is OK, we have got equipment that could, "distinguish between a packet's header and its communications payload, and make only the relevant header information available for recording or decoding."

Now, I assume the FBI was referring to its Carnivore equipment when it made that representation to the court. It actually made the same representation to the FCC. The reason I say this is the representation was critical, since both the FCC and the court noted that, "privacy concerns could be implicated if carriers were to give

to law enforcement packets containing both the addressing information and the content, when only the former"—that is, the addressing information—"was authorized."

Now, both the FCC and the court noted that CALEA imposes an affirmative duty on carriers to protect the privacy and security of communications not authorized to be intercepted. It also requires that they do not give law enforcement access to any communications or addressing information not covered by a court order.

I put all that as a basis to this question: do you believe that the way in which Carnivore operates gives law enforcement access to more than just the communications or addressing information covered in a court order? And if so, could it put the ISP in jeopardy of violating its duty under CALEA of protecting the privacy and security of communications not authorized to be intercepted?

Mr. KERR. The very simple answer to your question is that CALEA covers telecommunications carriers. The Internet service providers are not covered under CALEA. We have only used Carnivore in conjunction with the networks of Internet service providers.

We did, in fact, brief the standards committee for the companies and others involved in CALEA on the technology used in Carnivore in order that they would be aware of it as they develop a CALEA-based standard for telecommunications carriers using packet-switched networks. But there is no carryover between CALEA and what we have been talking about with Carnivore.

Senator LEAHY. Then what did the FBI mean, after the carriers had argued they couldn't separate packet headers and content—I am talking about telecommunications carriers when they argued that before the court, and the FBI said, well, that is OK, we have got equipment that could distinguish between packet headers and communications payload. Were they referring to Carnivore?

Mr. KERR. I think they were likely referring to Carnivore, but as a demonstration of a technical approach. To repeat, we have not used and don't expect to use Carnivore in a CALEA-covered intercept.

Senator LEAHY. Mr. Di Gregory, is that your understanding, too?

Mr. DI GREGORY. My understanding of what the FBI intends to use?

Senator LEAHY. Yes.

Mr. DI GREGORY. As I understand it, the FBI only intends to use Carnivore when the ISP is unable to provide the information or not willing to do so.

Senator LEAHY. Mr. Dempsey.

Mr. DEMPSEY. Well, Senator, Dr. Kerr is 100-percent correct when he says that CALEA does not apply to ISP's. And I have to say that was one of the smartest decisions that was made in the course of CALEA because implementing CALEA for the telephone companies has been a nightmare. It would be even worse trying to apply CALEA to the Internet and to ISP's.

But I think what the court and——

Senator LEAHY. It is a matter that we thought of at the time, as you recall. You were involved in some of that debate at that time.

Mr. DEMPSEY. Yes, I was, Senator. I take responsibility for all the mistakes we made there.

Senator LEAHY. No, no, no.

Mr. DEMPSEY. But keeping the Internet out was your and Congressman Edwards' decision, and it was a wise one, it turns out.

I think what the FBI was referring to was not Carnivore, per se, but this notion that we will let the technology make this distinction, this constitutionally-based distinction between content and something other than content.

We have a huge issue on the Internet about what about this transactional information? It is not just numbers dialed, and what should be the standard? Professor O'Neill referred to that. But assuming that you can distinguish between content and noncontent, the FBI said in the CALEA debate if the carriers can't separate it, give it all to us. Even under a pen register order, give us the whole packets and we, the FBI, will sort it out, and we will only keep what we are authorized to keep. We won't look at or keep what we are not authorized to keep. And if it is a pen register, content, we are not authorized to keep content. We have a machine, we have a capability to disregard that.

And what the court of appeals said, I think, is that is not good enough. The technology, the FBI, the Commission, the industry cannot modify the constitutionally-based rules for interception of content, and that in order to obtain and grab and look at and analyze and redirect content, you need a full probable cause-based order. And the FBI is using Carnivore under the pen register authority on the "trust us" standard that our technology will solve the problem of what is the distinction.

Now, Mr. Cerf has said it is very hard to distinguish between what is content and what is, "addressing information."

Mr. CERF. No, I didn't say it was hard to distinguish between the two. What I said is that you have to capture a lot before you can filter out the part which is considered header. Yes, you must capture it. Because of the structuring of the protocols, you have to capture essentially a lot of this piece of text before you can then find the part that you want to capture.

Mr. DEMPSEY. That poses huge constitutional problems.

Mr. CERF. Hang on, folks.

Senator LEAHY. Just a minute. To make sure I understand it, part of the problem is the "just trust us" standard, but it actually even goes beyond that, the fact that it is even being collected to begin with. Is that what you are saying, Mr. Dempsey?

Mr. DEMPSEY. Yes.

Mr. O'NEILL. If I may interject, this is part of the difficulty, I think, that Congress has to deal with. The fact that the Department of Justice—and I was very proud to have worked for the Department of Justice, and frankly in a lot of circumstances I much prefer the Department of Justice having any personal or private information about me than I do some industry groups or whether the ISP does. I mean, that is sort of my general default.

Part of the difficulty, though, is that the Department of Justice perceives its mission, and rightly so, as making sure that we are secure in our homes, preventing and stopping crime. In an effort to do that, what the Department has done, and rightly so, is to make sure that it stays technically relevant.

The Internet is a big change over the way people communicated in the past. In order for the FBI to be able to fight and deal with

the perceived threat and the actual threat, whether it is crime or international terrorism or what have you, it then develops software and it develops new and innovative approaches to collect information to continue doing what it has done in the past.

The difficulty and I think the challenge for Congress is to make sure that all of this technological innovation, all of these changes in the way that the FBI or Federal law enforcement assembles information— that someone is watching it. Judges frankly are in a very poor position to monitor this because judges frankly don't have the information available. They are only trained as lawyers. They are not in a situation like the U.S. Congress is to have people who are expert in these very complicated, and as we have seen from the discussion here today, very esoteric parts of technology.

Congress frankly is in the best position to be able to do that, and I think it is in Congress where the American people's trust has to reside to make sure that this just doesn't happen with nobody watching it, to make sure the Department of Justice isn't too good in fulfilling its mission, and that there is a public watchdog, namely the Congress, making sure that the appropriate balance between personal security and personal privacy is maintained.

Senator LEAHY. Well, I would agree there. I am happy we are having this hearing. Whether Congress is going to be adequate in this kind of oversight—I mean, we can be if we want to be. It is whether we set that as a priority, and you have worked up here and you know that there are a million things coming through at any given time, some substantive and some symbolic, and we tend to spend a lot of time on one or the other depending on what we are doing.

But the Sunday afternoon emergency court order is not going to be—the oversight is not going to be in the Congress, but it is going to be at the Department of Justice.

Mr. O'NEILL. But Congress should be setting the baselines.

Senator LEAHY. I agree.

Mr. O'NEILL. And once the baselines are set, then judges and the FBI and law enforcement can properly administer those baselines when they are out there in the field.

Mr. ROSEN. Can I just make a point on that?

Senator LEAHY. Well, Mr. Cerf had been trying to respond.

Mr. CERF. Only to support Mr. O'Neill's argument. It seems to me that it is inescapable that this technology will proliferate, not the Carnivore technology, the Internet technology, and that it will become the basis for most of our communications. Even if the other systems survive and persist, the Internet will carry television and telephony and radio, and so on.

So we need to learn how to deal with that. We need to deal with it in the context of the problems that the Justice Department and the FBI have, and other law enforcement people do, at the same time trying to protect individual rights to privacy. That balance has to be struck, and the terms and conditions for it surely lie squarely with our Congress.

Senator LEAHY. Mr. Rosen.

Mr. ROSEN. I wonder if I could make a concrete suggestion about striking that balance, to pick up on the suggestion. We have been focusing on the different standards for different forms of tech-

nology, for pen registers, for content, for header information. There is another approach that Congress took in the title III area which is really a model for protecting privacy and striking the balance that we are thinking about here, and that is limiting the most intrusive searches to the most serious crimes. A search of a diary, for example, might be reasonable in the context of the Unabomber, but not for a relatively trivial civil suit.

Now, there is a tendency, as you know, for the list of these crimes to expand exponentially. So originally the title III list was limited to really serious and violent crimes, and now it includes all felonies. But for searches of e-mail and for any content-based searches, you have the ability and the opportunity right now to really create a very limited number of crimes that can justify these searches.

And I think that citizens would just feel much more comfortable about having intimate information revealed when they know that there are violent and serious criminals involved than when they think that any of them may be caught up in a relatively trivial offense.

Senator LEAHY. What you are saying is the constitutional threshold remains the same, no matter what the crime is, but we will just simply say that constitutional threshold or not, you can only do these searches for certain types of crimes.

Mr. ROSEN. I guess the notion is the constitutional threshold is reasonableness, and a search is more likely to be reasonable if a serious crime is involved than if it is not. So in trying to substantiate that constitutional standard, just make sure that the list is limited when the searches are intrusive.

Senator LEAHY. Mr. Cerf, there is something I have always meant to ask you. Are you relation to the late Vincent Cerf?

Mr. CERF. To whom?

Senator LEAHY. The late Vincent Cerf.

Mr. CERF. Are you thinking of the late Bennett Cerf, perhaps?

Senator LEAHY. Well, there is also a Vincent Cerf.

Mr. CERF. There is a Vincent?

Senator LEAHY. Yes.

Mr. CERF. Gee, no, not that I am aware of. I am related to Bennett Cerf, both of them. One of them is my son and the other one, of course, is the former publisher at Random House. But I do not know Vincent Cerf.

Senator LEAHY. Bennett Cerf has the ability to come up with some of the wildest puns, as you probably know.

Mr. CERF. It is a genetic defect and it runs in the family.

Senator LEAHY. I have been accused of using some from years back.

Obviously, you are an acknowledged pioneer of the Internet, and you were kind enough to help out the Internet Caucus, and so on. You worked on ARPANet, which is the precursor to the Internet. You were there when the Internet was first discussed and began being developed into what it is today. I suspect that neither you nor anybody else could have envisioned just how quickly it has gone so far. You may have known that it would go like this, but the fact that it has moved so quickly.

But Congress also played an essential role. We funded not only ARPANet, but also the NSPNet and the backbone that led to the Internet. The reason I ask this is that some—I wouldn't suggest anybody on this committee, but some have poked fun at Al Gore on this issue. But I think they fail to acknowledge his role in Congress when he pushed for development and saw the potential of the Internet years ago when a lot of others didn't.

I remember back in the 1980's—and I remember this because his office was down the hall from mine—that then Senator Gore chaired a hearing that had the first ever live computer demonstration exhibiting the possibilities of a high-speed computer network. I know of nobody else who had done it up to that point.

So would you at least agree with me that the Vice President played a significant role in pushing for funding and development of what became the Internet, and may deserve some praise for his vision in that regard?

Mr. CERF. I would have to agree with that, Senator. The Vice President while he was Senator, in fact, was one of the first in this august body to realize that there might be something important about super computers and optical fiber and computer networking. He held a number of hearings, some of which had a direct impact and influence on legislation that supported the research that has led to the continued evolution of the Internet.

He has been a strong supporter, as I am sure you are aware, both in his senatorial role and as Vice President. And so I think it is quite proper for him to receive some credit for that interest and that support. I regret, as I suspect he does, the slip of the tongue that led him to characterize his role more broadly than I think it deserves.

Senator LEAHY. More broadly than he intended, too, I think.

Mr. CERF. I believe that is correct. On the other hand, I feel very strongly that he does deserve considerable credit for his consistent support for the Internet and related technologies.

Senator LEAHY. One of the national news media gave me what I thought was too flattering, but I am not going to ask for a retraction, profile referring to me as the Cyber Senator. I have got to admit that a lot of that interest came from then Senator Gore. When we were coming back from votes, he would start pounding my ear and then would grab me into office and keep on going until I agree that, yes, I would learn more about it, and then he would turn me loose.

Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Well, I want to thank all of you for being here today. This has been an excellent hearing. We have raised a lot of issues that are important. Naturally, all of us want to support law enforcement, it seems to me, in legitimate pursuit of those who are breaking the laws. I certainly do. On the other hand, we certainly want to be concerned about the privacy aspects of individual citizens in our society.

There are no easy answers to all of these very significant questions, but we are hopeful that you can continue to help us to understand this. So we will keep the record open for a week for any additional comments or statements anybody cares to make and any additional materials you would want to submit to us.

Senator LEAHY. Mr. Chairman, could I emphasize regarding submitting anything further, if you have further thoughts on that court of appeals case, I think it would be very helpful to both the chairman and myself if any of you would like to add to it. I mean, that is not a trick question in any way whatsoever, as you know. I am trying to figure out where it goes. So if you want to add something, if you want to ask your own question and answer it, please feel free to do so.

The CHAIRMAN. We will keep the record open for that.

We want to thank each and every one of you. You have been great here today, and this has helped us to understand this much better.

So with that, we will recess until further notice.

[Whereupon, at 12:31 p.m., the committee was adjourned.]

---

## QUESTIONS AND ANSWERS

### RESPONSES OF DONALD M. KERR TO QUESTIONS FROM SENATOR HATCH

*Question 1.* Is Carnivore set up to intercept all of the communications of all of the ISP Subscribers Within an ISP's Computer Network?

Answer 1. No. First of all, the FBI intentionally works closely with the computer network Administrator to decide on the best and most appropriate interception access point. This access point is determined with the specific purpose of finding the smallest segment within that ISP's computer network into which the criminal subject's communications traffic can be funneled, so as to minimize the amount of network traffic involved. Technically speaking, most ISPs can and do identify such a limited segment within the overall ISP network which contains the criminal subject's communications traffic. Second, the FBI uses a commercial device to attach Carnivore to, yet isolate it from, the network.

More to the point, the FBI has absolutely no intention of being put into a situation where Carnivore would have to interface with an entire ISP network. If someone had the erroneous idea that the FBI might desire to "capture" all such ISP network traffic—which it certainly does not want to and will not do—the Carnivore system could very quickly be overwhelmed with traffic. That is, Carnivore software is deployed on a standard PC and the largest hard drive that has been deployed is 18Gb. With the total traffic of many ISPs running at thousands of Mbps, even if this hard drive was storing only 100Mbps of network traffic, the Carnivore system would fill up in about three minutes.

The only exception to the aforementioned rule would be with regard to very small ISPs where all subscribers' communications traffic was traversing the same segment of the network as the criminal subject's traffic. Of course, under this unusual circumstances, Carnivore would, as it always does, filter out all of the traffic other than that of the criminal subject.

*Question 2.* Does the use of the Carnivore System legitimately raise the concern of Carnivore broadly conducting illegal searches as to other innocent, non-criminal subject subscribers' communications addressing information or communications content?

Answer 2. No. It is important to understand that Carnivore's filtering operates in stages—and that all filtering occurs exclusively within the "Carnivore box." Carnivore's first operation is exclusively to detect the criminal subject's identifying information. The first stage of filtering in the Carnivore system is to match (in purely binary computer code) the "pattern" of "1's" and "0's" in the computer bit stream that matches the subject's "pattern," based upon the criminal subject's identifying information, as set forth in the court order. So, in a very simplified example, with the filter exclusively set to detect the criminal subject's computer bit pattern "1100," if the first bit in the compute bit stream was an "0," Carnivore would automatically conclude that since "0" and "1" are not a match, that this circumstances does not meet the filter pattern criteria, and it would quickly move on to conduct the next pattern match effort. If the first digit is a match, Carnivore would then go to the next digit in the computer bit stream, and repeat the process, until an exact, complete match is arrived at.

Importantly, nothing happens at all, by way of any interception of communications content or acquisition of communications addressing information, unless and until the criminal subject's unique identifying information has been matched. Then, and only then, does Carnivore move on to the second stage of filtering, in terms of applying the appropriate filters required to filter either for communications addressing information acquisition or for full communications content interception, depending upon the particular authorization found within the court's order.

Finally, FBI personnel only receive and "see" the communications addressing information or communications content of the criminal subject, as appropriate—based upon the court's order—after all of the Carnivore filtering has been completed exclusively within the Carnivore box.

In short, Carnivore never conducts a search of the communications addressing information or communications content of any innocent, non-criminal subject at all. Indeed, even with the criminal's subject's communications traffic, Carnivore filters the criminal subject's "machine readable only" binary code exclusively within the box; and FBI personnel only obtain, in a humanly intelligible format—and "outside of the box"—the criminal evidence sought after Carnivore has completely concluded its programmed filtering efforts within the box.

*Question 3.* Does the FBI "view" computer network traffic as it passes through the Carnivore System?

Answer 3. No. First of all, Carnivore's filtering program renders Carnivore effectively blind to any network traffic other than that of the criminal subject, concerning whom a court has issued an order authorizing the acquisition of communications addressing and transactional information or the interception of communications content, all based upon identifying information unique to the criminal subject. Only such information about or communications content of the criminal subject is collected by Carnivore. Second, the computer network traffic passes through the Carnivore system at a speed far beyond human comprehension. The network traffic consists solely of a series of "machine readable only" 0's and 1's, flashing through Carnivore at a rate of 40 million "0"s/"1"s per second (and often at much higher speeds). Whenever any network traffic is stored on the Carnivore system, it remains in the same format of 0's and 1's; and, importantly, it is not turned into a format intelligible to humans until after it is transferred from the Carnivore system. Again, it bears repeating that Carnivore is a configurable system that will provide FBI personnel only that information that it has been programmed to deliver through its filtering—information that equates with the information authorized for interception/acquisition in the court's order.

*Question 4.* If the FBI were to conduct a pen register type investigation, wherein Carnivore would be programmed to only acquire the criminal subject's addressing information, and if the subject visited different web sites, would the carnivore system acquire information such as URL subdirectories? For example, if the subject went to Amazon.com to buy a book, would the FBI be able to tell what book he/she bought?

Answer 4. No. URL subdirectories are not acquired. The IP address and port number for Amazon.com alone would be acquired. Hence, the FBI would only know that the subject went to Amazon.com, and whether or not the subject established a "secure" connection (i.e., secure socket layer (SSL)).

*Question 5.* Can the FBI use Carnivore to intercept computer network communications other than e-mail?

Answer 5. Yes. Carnivore can be configured to intercept various types of computer network communications which match its filters. It has been used to intercept several protocols in the TCP/IP protocol suite (e.g., Telnet, FTP, IRC, and HTTP). Of course, in all instances, the appropriate legal process under Title III, FISA, or the ECPA would first have been obtained. If the electronic surveillance is for communications "content," a full Title III court order (probable cause showings and more) would be required.

*Question 6.* Does Carnivore interfere with the service or operations of an ISP computer network?

Answer 6. No. By design, Carnivore does not interfere with an ISP network.

First, the FBI works closely with the ISP computer network Administrator to decide on the appropriate interception access point. This access point is determined with the specific purpose of finding the smallest segment within that ISP's computer network into which the criminal subject's communications traffic can be funneled, so as to minimize the amount of network traffic involved. Then, importantly, a commercial device is used to attach Carnivore to, yet isolate it from, the network, such that, as a technological matter, it physically cannot and will not transmit anything whatsoever into the network or otherwise intrude into the network.

Second, by design, Carnivore's attachment to a network will not crash or interrupt network service. Recent comments reported in the media suggesting that Carnivore had interrupted or "crashed" the service or operations of a major ISP are completely false. In reality, a small loss of bandwidth did occur with the ISP in question, within only one segment of that ISP's network, when technicians from the ISP chose on their own to alter their software code to facilitate interception access. In fact, Carnivore was not even attached to the ISP network at the time when this ISP network problem arose.

*Question 7.* Does the Carnivore System use trojan horses or viruses to collect a criminal subject's communications content or addressing information?

Answer 7. No. The Carnivore system is totally passive. No software is added to a subject's computer.

*Question 8.* Once Carnivore has been deployed, can the filters be accessed and changed remotely?

Answer 8. Yes. Carnivore can be accessed remotely and the filters may be changed—but, (1) only a select few technical persons specially dedicated to the Carnivore program, (2) only when those few persons are privy to the specific dial-up access number, (3) only when those persons possess a hardware security device that is specifically required for remote access, and (4) only when such persons have the necessary two-tiered password access authority required.

Currently, within the FBI there are only a limited number of technically-trained personnel who implement the Carnivore program. As noted, the dial-up access is secured by both hardware and software protections, and any access, or attempted access, automatically generates a series of recorded logs which disclose precisely who, if anyone, has ever accessed Carnivore remotely and/or changed the filters in any given case. Importantly, any filter changes would be based upon some significant reason, such as a change in the legal process (e.g., moving from a pen register or trap and trace investigation to a full Title III, pursuant to obtaining a Title III court order), the termination of the surveillance period and Carnivore's attendant "shutdown," or for technical "trouble-shooting," if some technical problem or glitch arose.

Although investigative personnel have limited remote access capabilities for investigative purposes only—that is, to access the raw data that subsequently, through later processing, will constitute the evidence in the investigation—they are never given the second tier password required to access or change the Carnivore filter sets.

---

RESPONSES OF DONALD M. KERR TO QUESTIONS FROM SENATOR THURMOND

*Question 1.* Dr. Kerr, please explain the obstacles that law enforcement faces in getting information on electronic communications, especially with less encryption controls and with the increased use of digital messages.

Answer. As your question correctly suggests, technological obstacles to electronic surveillance are arising in the environment of electronic communications. These obstacles are varied and pose significant challenges to the law enforcement community's lawful conduct of court-ordered electronic surveillance.

In working with the vast array of large, medium, and small size Internet Service Providers (ISPs), we have encountered some unusual network-based obstacles. For example, even though the FBI always works very closely with such ISPs (both by desire and necessity) before we ever undertake an electronic surveillance effort, we have nonetheless encountered some unusual, non-standardized, and proprietary network protocols and other network controls within such ISP networks; and these complicate electronic surveillance efforts. Indeed, somewhat remarkably, we have found, in some instances, that a given ISP's most expert technical personnel themselves may not always be fully aware of, or conversant with, the protocols being utilized within their network and/or how they have been implemented. Such a situation can adversely impact upon the smooth effectuation of certain electronic surveillance orders.

In another vein, certain very high-speed electronic communications can likewise challenge, or threaten to undermine, the ability of law enforcement to fully and properly execute electronic surveillance court orders.

Finally, the use of encryption by criminal subjects (absent some lawful and efficacious law enforcement decryption capability), can threaten to undermine Federal District court electronic surveillance orders and the ability of law enforcement agencies to investigate and prevent serious acts of terrorism, espionage, and violent criminality.

As to the foregoing challenges and many others, the FBI historically has worked (and continues to work) closely with various business and technological components

within the electronic communications industry. and, by necessity, the FBI also steps in and develops its own tools, as necessary, when commercial tools are not available which fully meet legal, evidentiary, investigative, and operational requirements placed upon law enforcement's lawful conduct of electronic surveillance.

*Question 2.* Dr. Kerr, there has been considerable concern about the F.B.I. possibly using Carnivore to search randomly through all e-mails or other electronic communications that contain specific words or phrases like "bombs" or "drugs". Does the F.B.I. have the authority to gather intelligence on non-specific targets in this manner?

Answer 2. First of all, the FBI's Carnivore system simply does not work, as suggested by some, in a fashion of randomly searching through all E-mails or other communications that contain specific words or phrases like "bombs" or "drugs," etc. To the contrary, Carnivore is a "filtering" tool which the FBI has developed to carefully, precisely, and lawfully conduct electronic surveillance of electronic communications regarding a specific criminal subject—based upon that criminal subject's identifying information (e.g., his/her IP address)—occurring over a particular computer network, in complicance with the Constitution and the Federal electronic surveillance laws.

Whenever Carnivore is used, the FBI never deploys it without the cooperation and technical assistance of the ISP network technicians and/or engineers. Further, through working with the ISP, Carnivore is positioned and isolated in the network so as to focus exclusively upon just that small segment of the network traffic where the criminal subject's communications can be funneled. This is roughly analogous to using an electronic surveillance device only within in a single trunk or cable within a telephone network. Stated differently, and contrary to the assertions of some critics, Carnivore does not access 'in a big Brother mode, all subscriber communications throughout an ISP network.'

Carnivore's filtering operates in stages. Carnivore's first action is to filter only within a small portion of an ISP's network. Specifically, Carnivore filters binary code—streams of 0's and 1's that flow through an ISP network, for example, at 40 mega-bits per second, and often at much higher speeds. To visualize this, imagine a huge screen containing 40 million 0's and 1's flashing by on this screen for one screen for one second, and for one second only. Carnivore's first effort—entirely within the Carnivore box—is to identify within those 40 million 0's and 1's whether the particular identifying information of the criminal subject, such as his/her IP address, (for which a court order has been authorized) is there. If the subject's identifying information is detected, the packets of that criminal subject's communication associated with the identifying information that was detected, and those alone, are segregated for additional filtering or storage. However, it's very important to understand that all of those 40 million 0's and 1's associated with other communications are instantaneously vaporized after that one second. They are totally destroyed; they are not collected, saved, or stored. Hence, FBI personnel never see any of these 40 million 0's and 1's, not even for that one second.

After exclusively segregating the criminal subject's information for further machine processing, then a second stage of filtlering is employed. At this point, and again all within the Carnivore box, Carnivore checks its programming to see what it should filter and collect for processing. In other words, it determines, as required by the specific wording of the court order, if it's supposed to comprehensively collect communications content—in a full Title III or FISA mode—or, alternatively, whether it's only to collect pen register or trap and trace transactional and addressing information. Only that information specified in the court order is being collected and passed on to FBI personnel by Carnivore.

As to the second part of the question, the FBI does not have the authority to—certainly does not—gather intelligence on non-criminal targets in some broad brush manner. FBI electronic surveillance under title III and the ECPA focuses on gathering hard evidence about particular criminal subjects with regard to particular facilities being used by such criminal subjects and with reference to particular crimes and criminal communications, and with reference to identified co-conspirators.

*Question 3.* Dr. Kerr, what controls exist on the F.B.I. to insure that Carnivore is not misused for a fishing expedition or to obtain electronic communications that lie outside of the scope of a court order?

Answer 3. There are numerous legal, technological, and administrative controls that prevent the misuse of Carnivore for a fishing expedition or for intercepting communications outside the scope of the court order.

Legal Controls: First of all, the law itself is a powerful control to ensure that only properly authorized, lawful electronic surveillance occurs. The FBI certainly is of this opinion. As such, the FBI only conducts electronic surveillance—whether con-

ducted through the use of Carnivore or otherwise—pursuant to a lawful court order or lawful voluntary consent of a party to the communication. This has been the case since 1968, when the first Federal electronic surveillance laws were enacted in the Title III legislation. Importantly, the FBI has an outstanding record of compliance with the electronic surveillance laws since their enactment over 30 years ago. In addition, it is very noteworthy that the electronic surveillance laws contain stringent deterrents to unauthorized (illegal) electronic surveillance, including criminal (felony) and civil sanctions for any individual who violates the law. Further, under the Constitution, suppression of illegally obtained evidence (and fruits thereof) may be applied by Federal courts if electronic communications content is unlawfully intercepted.

Technological Controls: The Carnivore system, by design and functionality, is set up to establish an "audit record" for evidentiary purposes. Of course, a secondary aspect and value of this design and functionality would be to aid in the prevention of any potential infringement of privacy rights. Moreover, as you may be aware, Carnivore, by design, is a device which only functions to filter out. In its first filtering action, carnivore filters out anything not associated with the unique and specific identifier associated with a particular criminal subject's service, as identified in a given court order. Stated differently, Carnivore "ignores" and is "blind to" anything not associated with a criminal subject's unique identifier that relates to the specific authorization set forth in the court's order. In its second filtering action, Carnivore filters out content when the order is only for communications addressing and transactional information. Thus, as a special purpose electronic surveillance tool, Carnivore fundamentally and purposely works as a "filter." By contrast, Carnivore fundamentally and purposely does not work, descriptively speaking, as a "vacuum cleaner" which, by design, would purposely acquire electronic communications broadly and indiscriminately from all network users, including those of innocent subscribers. Hence, Carnivore's design does serve as an effective check against any potentiality of infringing upon privacy rights.

Adminstrative Controls: There are numerous administrative and criminal justice system-based controls which preclude the errant use of Carnivore, both in terms of internal and external oversight to control how Carnivore is being used at any point in time. To begin with, it should be emphasized that the FBI does not deploy or use Carnivore or any other non-consensual electronic surveillance tool in a vacuum. With regard to applications for pen registers or trap and trace devices, section 3121 of Title 18 of the United States Code prohibits Carnivore's use, as such a device, without a court order. In order to acquire a court order, the FBI may not act alone, but must seek the approval of an appropriate official within the Department of Justice. Section 3122 mandates that an "attorney for the government" be the applicant for a pen register or trap and trace device. Typically, this requires the approval of the Office of United States Attorney for the district in which the device is to be used. Of course, more stringent requirements, mandating high-level Department of Justice approval, are found in Title III/FISA provisions and practices controlling the interception of electronic communications.

Within the FBI itself, there are also a number of administrative, technological, and physical access controls which prevent the unauthorized use of any electronic surveillance tool, including Carnivore. First, as a general matter, all covert electronic surveillance equipment is carefully controlled and overseen within the FBI by FBI Headquarters program managers and by each field officer's Technical Advisor (TA). Second, with regard to Carnivore specifically, there are only a few Carnivore devices and only a limited number of FBI personnel who are trained to operate this special purpose tool, under FBI Headquarter's overnight. Third, to use Carnivore in any given case, such personnel must be privy to the specific access number for a targeted account number. Fourth, such personnel can use Carnivore only when they possess a hardware security device that is specifically required for access. And fifth, such personnel can use Carnivore only when they have the necessary two-tiered password access authority required.

Finally, if any FBI employee ever were to conduct such unlawful activity, he/she would be terminated from employment with the FBI. There is "zero tolerance" for any such illegal conduct within the FBI.

In sum, Carnivore has many legal, technological, and administrative controls. Such controls effectively act to prevent any "fishing expedition" or infringement of privacy rights when using Carnivore.

*Question 4.* Dr. Kerr, is Carnivore used in routine criminal investigations or is it limited to rare cases when the information cannot be obtained through the Internet Service Provider or another manner?

Answer 4. Carnivore has been used in important ECPA-based criminal investigations and in important FISA-based national security investigations. As noted in our

testimony, we have used Carnivore when the interception of electronic communications content or the acquisition of electronic communications addressing information could not be fully or properly effectuated by the Internet Service Provider (ISP) (with reference to legal, evidentiary, investigative, and operational requirements which need to be met) or when the ISP has indicated that it is ill-equipped to effect the interception or that it would be more efficient for the FBI to effectuate the order using Carnivore.

*Question 5.* Dr. Kerr, some have called upon the F.B.I. to release the source code for Carnivore. What impact would this have on the ability of Carnivore to operate?

Answer 5. To begin with, in enacting the first comprehensive U.S. electronic surveillance laws, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. 2510–2522, as amended, the Congress instituted a balanced regime which both affords clear statutory authority and Constitutionally-compliant procedures to enable law enforcement to lawfully conduct electronic surveillance pursuant to court order and which criminalizes the unauthorized conduct of electronic surveillance in order to underscore the Congress' intention of preventing unlawful searches and seizures and of preserving communications privacy. To advance both of these principles, the Congress also crafted Title III provisions to prevent the proliferation of surreptitious electronic surveillance interception devices. *See* 18 U.S.C. 2512 (Manufacture, distribution, possession, and advertising of wire, oral, and electronic communication intercepting devices prohibited). The only two categories of users exempted under Section 2512 are providers of wire or electronic communication service, with regard to equipment utilized by them in the normal course of providing their service, and governmental officials, with regard to equipment utilized by them in the normal course of carrying out governmental activities.

Similarly, there are statutory and regulatory U.S. export control regimes which govern the export of electronic surveillance-related equipment (e.g., the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations, and the Export Control Act, as implemented by the Export Administration Regulations). Depending upon the type of electronic surveillance equipment involved, one or both of these regimes will likely govern the export of electronic surveillance equipment.

In short, electronic surveillance equipment generally, and that used by the FBI in particular (at least that electronic surveillance equipment used in covert, nonconsensual efforts—i.e. surreptitious electronic surveillance devices) is treated as sensitive, at a minimum. In many cases, such equipment may also be classified. Hence, in light of the above, and as a starting point, the FBI is concerned about the legal and policy constraints associated with the disclosure of such electronic surveillance equipment, including its software.

With regard to Carnivore, and again in light of the above laws, controls, and constraints, we believe that it would be improper to disclose to the public generally the source code of Carnivore. The source code, after all, is for a special purpose surreptitious electronic surveillance system which should be treated with circumspection. Public disclosure of the source code could lead to the unintended and harmful effect of facilitating unauthorized, and hence unlawful, electronic surveillance. Further, it may be that disclosure could inform the criminal community about aspects of Carnivore that might suggest some potential for circumvention.

However, as you may be aware, the FBI will disclose the Carnivore source code to the independent, outside review team which the Attorney General has called for (the Illinois Institute of Technology and Research Institute (IITRI)) in a controlled environment and under controlled circumstances, in order to give assurance to the public that Carnivore operates properly and lawfully, as the FBI claims it does.

*Question 6.* Dr. Kerr, do you think the name Carnivore has contributed to public perceptions about the program being extremely intrusive?

Answer 6. It's probably fair to say that the name "Carnivore" has unintendedly and unhappily lent itself to some negative comments by those who have not understood Carnivore's actual use, functionality, and core purpose in making electronic surveillance efforts more—not less—surgical and precise. As noted in our testimony, in a number of regards, Carnivore is superior, as an electronic surveillance tool, to the "sniffers" that are sold commercially and often used by ISPs for network troubleshooting and management (such sniffers were never intended for use as a law enforcement electronic surveillance tool). Indeed, in the furor, the public appears to have lost sight of the core fact that the FBI has spent considerable time, money, and energy in trying to develop an electronic surveillance tool which better meets the dictates of the Constitution and the Federal electronic surveillance laws.

RESPONSES OF DONALD M. KERR TO QUESTIONS FROM SENATOR LEAHY

*Question 1.* By letter dated August 16, 2000, the FBI informed me that "Carnivore is only used in those small number of instances when an ISP cannot on its own deliver what the court order instructs," suggesting that Carnivore is an investigative tool of last resort. Others have expressed the view that Carnivore should be a tool of first resort because the responsibility for executing court orders for electronic surveillance and protecting privacy rights is best discharged by the Department of Justice, not private ISPs. What is your view?

Answer 1. In the past, the FBI's decision to use Carnivore or to permit an ISP to implement a court-authorized electronic surveillance order for either the full interception of electronic communications content or for the acquisition of electronic communications addressing and transactional information within an ISP's network has been decided on a case-by-case basis. Given the complexities and the great number of variables related to any given court-authorized electronic surveillance technical effort within an ISP network, the FBI has always viewed such electronic surveillance efforts from a tactical and effectiveness perspective. Central factors considered by the FBI in making determinations have been the ISP's ability to implement a particular order fully, properly, securely and in a timely manner. If the ISP can meet these requirements, we would normally let the ISP implement the order.

Further, it is important to remember that both as a technological and practical matter, the FBI's conduct of electronic surveillance within such ISP's computer network always requires a cooperative and collaborative effort between the ISP and the FBI. This is so because an ISP's network administrators and engineers are really the only ones possessing the knowledge required as to their network to identify within it the transmission pathway(s) of a particular criminal subject, the best access vantage point(s), the protocols being used, etc.—all of which are required to effectively execute a surveillance order.

Hence, the FBI believes the best approach will continue to be a case-by-case approach, based upon considerations such as those outlined above.

*Question 2.* The FBI has testified that Carnivore has been used, as of September 6, 2000, in approximately 25 instances and that "in many instances, ISPs, particularly the larger ones, maintain certain technical capabilities which allow them to comply, or partially comply, with court order."

*A.* Is it fair to say the majority of court orders for electronic surveillance of Internet communications or source and destination information of Internet communications are executed by ISPs without the use of Carnivore?

*B.* Since the FBI employs Carnivore only on rare occasions when its use is necessary, should the FBI retain the right to use Carnivore in all cases?

*C.* Should the government be required to make a showing that use of Carnivore is necessary and obtain court permission before using this tool?

*D.* Would concern about abuse of Carnivore be allayed if its use were limited to circumstances when a court has granted explicit permission for the electronic surveillance order to be executed by law enforcement on the ISP's premises?

Answer 2 A and B. Again, owing to a number of factors and variables, as outlined above in Answer #1, and their interrelationship, we cannot give an unqualified answer. Generally speaking, certain very large ISPs do tend to have greater electronic surveillance capabilities than the small ISPs. For example, if the electronic surveillance order were for the interception of E-mail content, certain ISPs could "clone" the E-mail and accomplish, or very substantially accomplish, such an interception effort. When the ISP can meet electronic surveillance requirements, we have permitted the ISP to effect the surveillance effort. However, since most ISPs have developed with little emphasis being placed on conducting electronic surveillance for law enforcement, and since the "tools" that they might typically resort to in order to effect such efforts (e.g., "commercial sniffers") were never designed for such a law enforcement electronic surveillance purpose, surveillance shortfalls can occur. By comparison, the FBI's Carnivore system was specially designed to effect such surveillances. In this regard, it bears noting that, when an ISP does lack the capability to implement a court order fully, properly, securely, and in a timely manner, the ISP usually is the first to recognize that it is more effective for the FBI to use its electronic surveillance tools.

Given the different and sometimes unique factors and variables that arise from case to case, as noted above, we believe that the FBI must retain the right to use its electronic surveillance equipment in order to ensure that electronic surveillance orders can be implemented fully, properly, securely and in a timely manner. However, in the rare instances where a dispute may arise between the government and the ISP, as with any matter in contention, resolution of such matter is through the

courts, with a judge or magistrate resolving it. Resolution is never dictated unilaterally by the government, much less by the FBI.

Answer 2 C and D. We believe, based upon different factors and variables, as outlined above, as well as our past experience in this area, that the best course is one where the ISP and the FBI work closely together in a consultative, cooperative, and collaborative fashion to implement a particular electronic surveillance order in the best way possible, so that the court's order is properly implemented and not frustrated. The technical and administrative staff of an ISP is best positioned, in concert with law enforcement, to make complex technological judgments, which often arise only after the court issues its order. Relatedly, the FBI does not have the resources that would be required to initiate in-depth discussions with all the ISPs (some in industry estimate the number of ISPs to be in the thousands) that conceivably could be involved in a potential future court-ordered electronic surveillance interception (with an eye to pre-determining what technological approach might be best) prior to the time when an actual and specific order may in fact be issued by a particular court. Further, and as indicated above, such pre-determination could, at best, only be general and tentative in nature since, as noted, many different technological variables and factors come into play, and, importantly, they change over time as the ISPs' networks change over time. Thus, especially in fast-paced investigations where time is of the essence, such as in computer hacker cases, to require in advance a specialized demonstration of need to a court in order to utilize Carnivore, as suggested, would impose very problematic procedural delays. Neither FBI nor ISP engineers would be in a position to make a final determination until after a particular order authorizing interception or acquisition of particular information had been issued at a particular juncture in time with reference to the then technological state of the given ISP's network.

As to the issue of concern about abuse, as noted in our hearing testimony, Carnivore has a built-in audit record. This audit record feature was designed into Carnivore for the purpose of making a permanent record as to the particular filter settings that have been used in each case with Carnivore—and hence what information has been acquired by Carnivore—at any point in time. Thus, this Carnivore feature creates a record to afford assurance to any interested party (FBI managers, Offices of the United States Attorney, U.S. District Courts, juries, criminal defendants, and defense counsel) as to precisely what Carnivore is or is not acquiring at any point of time in each investigation. Also, as with any type of electronic surveillance within any service provider network (wire or electronic), the criminal and civil penalties within our electronic surveillance laws, along with close DOJ and FBI administrative oversight, prevent misuse of electronic surveillance. Indeed, the FBI has an outstanding record of compliance with the electronic surveillance laws since their enactment over 30 years ago.

*Question 3.* The FBI and Department of Justice have asserted that Carnivore is the functional equivalent of pen register and trap-and-trace devices used on telephone lines. The Supreme Court held in *Smith* v. *Maryland,* 442 U.S. 735 (1979), that telephone callers do not have an expectation of privacy in dialed numbers used in placing a call since such numbers are necessarily divulged to a telephone company, which makes a permanent record for purposes of billing operations and maintenance of the service. The Court specifically distinguished such dialed numbers from "content," which are protected by the Fourth Amendment.

*A.* An Internet user may go to a particular URL that specifies not only the computer on the Internet on which a particular document can be found, but also the directory in which the document is located, the file name of the document and the page within the document that the user seeks and retrieves. Does such a URL or "Internet address" contain more or less information about the subject of a communication than a dialed telephone number?

*B.* Is Carnivore capable of intercepting information about a specific URL searched by an Internet user who is the subject of a pen register order? If so, at what point in the searching, or addressing, information would the Justice Department believe that the line has been crossed into "content"?

*C.* Is Carnivore capable of intercepting information about all the URLs visited by an Internet user who is the subject of a pen register order during a particular session?

Answer 3 A, B, and C. To clarify, a Uniform Resource Locator (URL) is simply an electronic Internet Protocol (IP) domain name address (e.g., xyzcorp.com). Further, also riding underneath the alphabetic URL address is a numeric address associated with the server that is supporting the contacted URL. Accordingly, when, pursuant to a pen register court order, the FBI uses Carnivore and acquires URL address information that is all that is being acquired—i.e., the fact that a criminal

subject has electronically connected to a given URL address. As such, the URL address information does not include any subdirectory or any other information about the site. In such a case, the FBI would only know that the criminal subject had contacted the xyzcorp.com site and whether or not his/her computer had established a "secure" connection (i.e., secure socket layer (SSL))—no more. Hence, in light of the foregoing, we believe that such URL information is essentially identical to a telephone number within a telephone network that a criminal subject may dial. Thus, it is worth noting that a Carnivore-based pen register would provide the FBI with virtually the same information as a telephone pen register would, i.e., the telephone number dialed by the criminal subject reflecting that a communication to XYZ Corp. had occurred. No "content" information (substance, purport or meaning) is gleaned from either type of pen register as to the nature of the call.

*Question 4.* Under current law, a judge must issue a pen register order upon a prosecutor's certification that the information likely to be obtained is relevant to an ongoing investigation. I have proposed in the E–RIGHTS Act, S. 854, that the law be changed to authorize a judge to issue such an order upon finding that the prosecutor has shown that the information is likely to be relevant. The Administration has proposed a similar change in current law. By contrast, Professor O'Neill suggested at the hearing that Congress should consider whether all Internet trap and trace orders should issue only on the basis of a judicial finding that probable cause exists to believe that a target has or is about to commit a crime. Representatives Canady and Hutchinson have proposed a bill that would require a prosecutor seeking e-mail source/destination information to show specific and articulable facts reasonably indicating that a crime has been, is being or will be committed, plus a showing of relevance of the information sought to investigation of that crime. A bill sponsored by Representatives Barr and Emerson would apply that standard to all pen registers and traps-and-traces whether or not they would identify e-mail addresses. What modifications, if any, to the existing standard for pen registers and traps-and-traces do you favor?

Answer 4. We believe now, as we did in 1986 when agreement was reached in the Congress (and amongst all of the interested parties) in enacting the Electronic Communications Privacy Act of 1986 (ECPA), that the current (ECPA) standard with regard to the use of pen registers and traps and traces is appropriate for the acquisition of non-content-based pen register-related addressing and transactional information. On March 28, 2000, Director Freeh testified in support of S. 2092, a bi-partisan bill co-sponsored by Senator Schumer and Senator Kyl. The FBI believes S. 2092 maintains the appropriate 1986 ECPA standard with regard to the acquisition of non-content-based "addressing and routing" information while rendering the pen register statute technologically neutral.

*Question 5.* According to the FBI, Carnivore operates by sifting through network traffic where a subject's communications are expected to be found "roughly analogous to using an electronic surveillance device . . . on a single trunk or cable within a telephone network." In your view, does the manner in which Carnivore operates give law enforcement access to more than just the communications or addressing information covered in a court order and, if so, would a telecommunications carrier that is also serving as an ISP be put in jeopardy of violating its duty under CALEA of protecting "the privacy and security of communications . . . not authorized to be intercepted"? (47 U.S.C. 1002).

Answer 5. As to the first part of your question, the way Carnivore operates, as described at some length in Answer #9(B), below, does not give the FBI more than the communications or addressing information covered by a particular court order. As to the second part of your question, no, we believe that the CALEA directive concerning protecting "the privacy and security of communications not authorized to be intercepted" applies only to those technological approaches and technical requirements that are developed to provide solutions covered by CALEA.

*Question 6.* Professor O'Neill has suggested a number of steps to be taken by Congress to address questions raised by Carnivore, including obtaining answers to the following questions:

*A.* Please explain the legal authority for law enforcement to insist that an ISP install Carnivore?

*B.* Can Carnivore be easily defeated by encryption software or does this tool capture IP addresses that are more difficult to encrypt than the contents of messages?

Answer 6A. The primary legal authority for the FBI and the United States Attorney's Office requiring that an ISP cooperate in installing Carnivore would be to avoid the "frustration" of a particular court order. The prospect of frustration, in the first instance, would stem from an ISP's inability to implement a given order fully, properly, securely, and in a timely manner. Both the Title III and the pen register/

trap and trace statutes have specific "assistance" provisions addressed to, among others, "providers of wire or electronic communications service" for the purpose of avoiding frustration of court orders. The statutes state that such providers "shall furnish . . . [the] investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish [the Title III interception or the installation of the pen resister]." Accomplish necessarily means fully accomplish, such that valuable evidence is not lost and such that its accuracy/integrity is not challengeable. Second, it is to be done securely. And third, as indicated by the statutory language ("forthwith"), a service provider must be able to assist very promptly. 18 U.S.C. 2518(4), 18 U.S.C. 3124, respectively. The language in the "assistance order" issued by the judge or magistrate usually mirrors the statutory language exactly.

As emphasized in the FBI's testimony, anytime the FBI has a surveillance order where an ISP can (1) fully and properly accomplish the surveillance, (2) do it securely, (3) do it very promptly, the FBI has been content to permit the ISP to implement the order. However, noting the foregoing statutory and court order language, the FBI and the United States Attorney's Office legitimately and properly could insist upon an ISP's cooperation with regard to the use of FBI electronic surveillance equipment (whether it be Carnivore or other equipment) that would work to execute an order fully, properly, securely, and in a timely manner, whenever the ISP does *not* have the capability to satisfy such requirements. Of course, if there were to be a dispute in this regard between the FBI and the ISP, as with any matter in contention, the resolution of the matter would be through the court, with a judge or magistrate resolving the issue. Resolution would not be dictated unilaterally by the government, much less by the FBI.

Answer 6B. Carnivore was not designed to address encryption. Any encryption that was encountered would require decryption through other means or devices.

*Question 7.* At the hearing, Dr. Kerr testified that Carnivore had recently been updated and improved. Presumably, the FBI will continue to update and improve Carnivore even after the independent technical review for which the Attorney General is now arranging. According to the FBI, one way to monitor Carnivore's use and modifications after conclusion of the technical review is by a so-called "audit trail" which allows a defendant to see how the FBI conducted a Carnivore search keystroke-by-keystroke. If the search was improperly conducted, the defendant might have grounds for suppression. Even if the audit trail operates as advertised, however, it will only be available to criminal defendants against whom prosecutors seek to introduce evidence obtained by Carnivore. How do we assure the law-abiding public after the anticipated technical review that Carnivore will not infringe on privacy rights? Should Congress consider an independent monitor for that purpose?

Anwser 7. There are numerous legal, technological, and administrative controls in place that prevent the misuse of Carnivore and any infringement upon privacy rights.

Legal Controls: First of all, the law itself is a powerful control to ensure that only properly authorized, lawful electronic surveillance occurs. The FBI certainly is of this opinion. As such, the FBI only conducts electronic surveillance—whether conducted through the use of Carnivore of otherwise—pursuant to a lawful court order or lawful voluntary consent of a party to the communication. This has been the case since 1968, when the first Federal electronic surveillance laws were enacted in the Title III legislation. Importantly, the FBI has an outstanding record of compliance with the electronic surveillance laws since their enactment over 30 years ago. In addition, it is very noteworthy that the electronic surveillance laws contain stringent deterrents to unauthorized (illegal) electronic surveillance, including criminal (felony) and civil sanctions for any individual who violates the law. Further, under the Constitution, suppression of illegally obtained evidence (and fruits thereof) may be applied by Federal courts if electronic communications content is unlawfully intercepted.

Technological Controls: As you note in your question, the Carnivore system, by design and functionality, is set up to establish an "audit record" for evidentiary purposes. Of course, a secondary aspect and value of this design and functionality would be to aid in the prevention of any potential infringement of privacy rights. Moreover, as you may be aware, Carnivore, by design, is a device which only functions to filter out. In its first filtering action, Carnivore filters out anything not associated with the unique and specific identifier associated with a particular criminal subject's service, as identified in a given court order. Stated differently, Carnivore "ignores" and is "blind to" anything not associated with a criminal subject's unique identifier that relates to the specific authorization set forth in the court's order. In its second filtering action, Carnivore filters out content when the order is only for

communications addressing and transactional information. Thus, as a special purpose electronic surveillance tool, Carnivore fundamentally and purposely works as a "filter." By contrast, Carnivore fundamentally and purposely does not work, descriptively speaking, as a "vacuum cleaner" which, by design, would purposely acquire electronic communications broadly and indiscriminately from all network users, including those of innocent subscribers. Hence, Carnivore's design does serve as an effective check against any potentiality of infringing upon privacy rights.

Administrative Controls: There are numerous administrative and criminal justice system-based controls which preclude the errant use of Carnivore, both in terms of internal and external oversight to control how Carnivore is being used at any point in time. To begin with, it should be emphasized that the FBI does not deploy or use Carnivore or any other non-consensual electronic surveillance tool in a vacuum. With regard to applications for pen registers or trap and trace devises, section 3121 of Title 18 of the United States Code prohibits Carnivore's use, as such a device, without a court order. In order to acquire a court order, the FBI may not act alone, but must seek the approval of an appropriate official within the Department of Justice. Section 3122 mandates that an "attorney for the government" be the applicant for a pen register or trap and trace device. Typically, this requires the approval of the Office of the United States Attorney for the district in which the device is to be used. Of course, more stringent requirements mandating high-level Department of Justice approval, are found in Title III/FISA provisions and practices controlling the interception of electronic communications.

Within the FBI itself, there are also a number of administrative, technological, and physical access controls which prevent the authorized use of any electronic surveillance tool, including Carnivore. First, as a general matter, all covert electronic surveillance equipment is carefully controlled and overseen within the FBI by FBI Headquarters program managers and by each field office's Technical Advisor (TA). Second, with regard to Carnivore specifically, there are only a few Carnivore devices and only a limited number of FBI personnel who are trained to operate this special purpose tool, under FBI Headquarter's oversight. Third, to use Carnivore in any given case, such personnel must be privy to the specific access number for a targeted account number. Fourth, such personnel can use Carnivore only when they possess a hardware security device that is specifically required for access. And fifth, such personnel can use Carnivore only when they have the necessary two-tiered password access authority required.

Finally, if any FBI employee ever were to conduct such unlawful activity, he/she would be terminated from employment with the FBI. There is "zero tolerance" for any such illegal conduct within the FBI.

In sum, Carnivore has many legal, technological, and administrative controls. Such controls effectively act to prevent any infringement of privacy rights when using Carnivore.

As to the second part of your question, we believe that it would be imprudent for the Congress to contemplate as a course of action, in the context of the concerns expressed with regard to Carnivore, the establishment of an outside "independent monitor." There are a number of reasons why resort of such an independent monitor would be problematic, including, but not necessarily limited to, the following. First, there is a likely separation of powers issue with regard to the Executive Branch's Constitutionally-reserved right to fashion and utilize proper sources and methods in order to lawfully and fully execute warrants and court orders (including electronic surveillance orders). Second, as a general proposition, such an approach, if adopted, could give rise to the unintended result of casting the independent monitor in the awkward role of being a sort of "electronic surveillance technology police," a role particularly ill-suited to a complex environment of fast-moving technology and the associated need for nimble electronic surveillance response. Third, it would appear to use that for this approach to really work the independent monitor may also have to assume an unprecedented and ongoing supervisory role throughout the duration of an execution of a given court-ordered surveillance. As can be seen, significant philosophical and legal including Constitutional) problems arise with the prospect of having the government itself "surveilled" by an "independent monitor" as the FBI proceeds to lawfully execute a warrant or court order.

If assuring the propriety of FBI surveillance is the core issue, as noted immediately above, other effective checks and balances are in place. Also, although the focus of the instant suggestion pertains to Carnivore, as a matter of precedent, the notion associated with using an independent electronic surveillance monitor could in principle be applied to every piece of electronic surveillance equipment that might be designed and used by the FBI, by other Federal law enforcement and/or security agencies, and by State and local law enforcement agencies. We would strongly recommend against pursing such an approach.

*Question 8.* Some universities interested in responding to DOJ's solicitation of bids to conduct the independent technical review of Carnivore have reportedly criticized certain terms of a non-disclosure agreement which the chosen contractor would be required to sign. One witness at the hearing said that the FBI would be a party to the required agreement. Please provide a copy of the non-disclosure agreement, identify the terms that have been criticized and explain why they are necessary.

Answer 8. Attached at the end of this document is a copy of the "Sensitive Information Nondisclosure Agreement" (NDA) executed by the Carnivore review team contractor.

In the recent Senate hearing on Carnivore, Mr. James Dempsey cited a USA Today On Line story where certain universities reportedly had indicated a reluctance to participate. One point noted in the story was that "Universities and any other contractors must agree not to publish anything the government deems sensitive." Hence, it appears, based upon the USA Today's characterization, that the university community's objection is more global as to the general proposition of not disclosing "sensitive" information as opposed to any particular "term" or provision in the NDA.

To begin with, the attached NDA is derived from a standard FBI NDA form (FD 857) which the FBI sues when sharing sensitive information with outside entities such as contractors and other persons. Such NDAs are also typically included in FBI/DOJ federal contracting. In the instant case, the FBI worked with the Carnivore review team contractor, the Illinois Institute of Technology Research Institute (IITRI), in formulating final NDA language which satisfied the contractor and which did not stifle the full review of Carnivore by the contractor.

As to the second part of the question, electronic surveillance equipment, including software, *is* sensitive and, under law, information about it is strictly controlled and constrained.

As you are aware, in enacting the first comprehensive U.S. electronic surveillance laws, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III), 18 U.S.C. 2510–2522, as amended, the Congress instituted a balanced regime which both affords clear statutory authority and Constitutionally-compliant procedures to enable law enforcement to lawfully conduct electronic surveillance pursuant to court order and which also criminalizes the unauthorized conduct of electronic surveillance in order to underscore the Congress' intention of preventing unlawful searches and seizures and of preserving communications privacy. To advance both of these principles, the Congress also crafted a particular Title III provision to prevent the proliferation of surreptitious electronic surveillance interception devices. *See* 18 U.S.C. 2512 (Manufacture, distribution, possession, and advertising of wire, oral, and electronic communication intercepting devices prohibited). The only two categories of users exempted under Section 2512 from using such devices are providers of wire or electronic communication service, with regard to equipment utilized by them in the normal course of providing their service, and governmental officials, with regard to equipment utilized by them in the normal course of carrying out governmental activities.

Similarly, there are statutory and regulatory U.S. export control regimes which govern the export of electronic surveillance equipment (e.g., the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations, and the Export Control Act, as implemented by the Export Administration Regulations). Depending on the type of electronic surveillance device involved, one or both of these regimes govern the export of electronic surveillance equipment.

In short, electronic surveillance equipment generally, and that used by the FBI in particular (at least that electronic surveillance equipment used in covert, nonconsensual efforts—i.e. surreptitious electronic surveillance devices) is treated as sensitive, at a minimum. In many cases, such equipment may also be classified. Hence, in light of the above, the FBI is concerned about the legal and policy constraints and controls that would conflict with the open-ended public disclosure of such electronic surveillance equipment, including its software.

With regard to Carnivore, and again in light of the above laws, controls, and constraints, we believe that it would be improper to disclose to the public generally the source code of Carnivore. The source code, after all, is for a special purpose surreptitious electronic surveillance system which should be treated with circumspection. Public disclosure of the source code could lead to the unintended and harmful effect of facilitating unauthorized, and hence unlawful electronic surveillance. Also, it may well be that disclosure could inform the criminal community about aspects of Carnivore that might suggest some potential for circumvention.

However, as you are aware, the FBI will disclose the Carnivore source code to the IITRI review team under controlled circumstances in order to give assurance to the

public that Carnivore operates properly and lawfully, as the FBI claims it does. In so sharing such sensitive information, it is altogether appropriate that an NDA be utilized to protect the information. It is important to note, however, that nothing in the NDA can reasonably be read to prohibit or stifle the disclosure of information of findings, potentially critical of Carnivore or the FBI, to the Attorney General and the Department of Justice. In conclusion, the testimony of the respected Internet expert, Mr. Vint Cerf (who previously was briefed as to Carnivore and who signed an NDA), is worth noting in this regard. At the hearing, Mr. Cerf testified, "May I just interject that I agreed to sign the nondisclosure on the principle that when you're dealing with surveillance just as you would with other intelligence situations, sources and methods are always a sensitive issue."

*Question 9.* In the D.C. Circuit Court of Appeals recent decision on the FCC's implementation of CALEA (the "Communications Assistance for Law Enforcement Act"), the Court agreed with the FCC that under a standard adopted by telecommunications carriers for packet-switched networks, the carriers could provide both packet headers and the content, or "payload," to law enforcement. Carriers argued that technically they could not separate the two, while the FBI contended that it had equipment which could "distinguish between a packet's header and its communications payload and make[] only the relevant header information available for recording or decoding."

*A.* Was the FBI referring to its "Carnivore" equipment when it made this representation to both the FCC and the Court?

*B.* The FBI's representation was critical, since both the FCC and the Court noted that "privacy concerns could be implicated if carriers were to give to [law enforcement] packets containing both [the addressing information and the content] when only the former was authorized." When Carnivore is installed, is the ISP essentially giving law enforcement the entire traffic flow over that particular part of the network, including both addressing information and content of packets?

*C.* The FBI testified at the hearing that CALEA does not apply to ISPs. In fact, CALEA, by its terms, applies only to telecommunications carriers. Are there telecommunications carriers that are also ISPs? If so, please provide examples.

*D.* Should the privacy concerns expressed by the Court for packet-switched networks apply only to telecommunications carriers, as defined in CALEA, or do those concerns apply more broadly to ISPs?

Answer 9A. The reference in question was not to Carnivore. The representation was generic as to what the FBI believes can be designed to separate communications from call-identifying information.

Answer 9B. First, we would like to clarify a couple of points included in the opening paragraph of this CALEA-related question. One point is that the FBI has asserted in its FCC filings regarding CALEA that, as a matter of technology, it believes that devices can be designed that would be capable of separating the communications content from the communications call-identifying information. A second point is that, assuming the availability of such devices, any entity, including a "telecommunications carrier" under CALEA, presumably could avail itself of them and *use any such device itself.*

As to your specific question, "[w]hen Carnivore is installed, is the ISP essentially *giving* law enforcement *the entire traffic flow over that particular part of the network, including both addressing information and content of packets?*" (emphasis added), some clarification is in order. First, what an ISP "gives" to law enforcement, when it identifies a "particular part of [its] . . . network]" is a vantage point through which "access" can be achieved as to the *specific* communications traffic of a *particular* criminal subject, based exclusively upon that particular criminal subject's *unique* identifying information.

Further, to better respond to your question, it is useful to explain more particularly how Carnivore actually works. As we set forth in our statement for the record, Carnivore is a special purpose electronic surveillance system which, pursuant to an appropriate court order or lawful consent, is used to acquire or intercept a criminal subject's communications addressing and transactional information or communications content, respectively, *based exclusively upon filtering that segregates a criminal subject's communications traffic based upon his/her unique identifying information (e.g., his/her E-mail address, IP address).* Carnivore does *not* acquire or intercept any innocent, non-criminal subject's communications addressing or transactional information or communications content.

Moreover, it is important to understand that Carnivore's filtering operates in stages—and that all filtering occurs exclusively within the "Carnivore box." As noted, Carnivore's first operation is exclusively to detect the criminal subject's identifying information. The first stage of filtering in the Carnivore system is to match

(in purely binary computer code) the "pattern" of "1's" and "0's" in the computer bit stream that matches the criminal subject's identifying information "pattern"—which identifying information is set forth in the court's order. So, in a very simplified example, with the filter exclusively set to detect the criminal subjects's computer bit pattern "1100," if the first bit in the computer bit stream was an "0," Carnivore would automatically conclude that since "0" and "1" are not a match, that this circumstance does not meet the filter pattern criteria, and it would quickly move onto conduct the next pattern match effort. If the first digit is a match, Carnivore would then go to the next digit in the computer bit stream, and repeat the process, until an exact, complete match is arrived at.

Importantly, nothing happens at all, by way of any interception of communications content or acquisition of communications addressing information, unless and until the criminal subject's unique identifying information has been matched. Then, and only then, does Carnivore move on to the second stage of filtering, in terms of applying the appropriate filters required to filter either for communications addressing information acquisition or for full communications content interception, depending upon the particular authorization found within the court's order. Finally, FBI personnel only receive and "see" the communications addressing information or communications content of the criminal subject, as appropriate—based upon the court's order—after all of the Carnivore filtering has been completed exclusively within the Carnivore box. Indeed, whenever any network traffic is stored on the Carnivore system, it remains in the same format of 0's and 1's; and, importantly, it is not turned into a format intelligible to humans until after it is transferred from the Carnivore system.

In sum, Carnivore *never* conducts a search of the communications addressing or transactional information or communications content of any innocent, non-criminal subject at all. Indeed, even with the criminal subject's communications traffic, Carnivore filters the criminal subject's "machine readable only" binary code exclusively within the box; and FBI personnel only obtain, in a humanly intelligible format—and "outside of the box"—the appropriate criminal evidence sought after Carnivore has completely concluded its programmed filtering efforts within the box.

Answer 9C As implied in your question, and as anticipated in CALEA, a communications service provider's business could offer both telecommunications services and information services. Examples of such companies are AT&T and MCI WorldCom. CALEA's coverage with reference to the definition of "telecommunications carrier" "does not include (i) persons or entities *insofar as they are engaged in providing information services* (emphasis added). " See 47 U.S.C. 1001(8)(C).

Answer 9D. The D.C. Court of Appeals decision pertained to the actions taken by the Federal Communications Commission in light of its CALEA-implementing Third Report and Order, and with reference to actions taken by the Telecommunications Industry Association in its CALEA-implementing J-Standard. The court's decision, hence, was CALEA-centric. The FBI and the Department of Justice (DOJ) have articulated their perspectives with regard to packet mode communications at some length in their comments before the FCC (see FBI and Department of Justice "Comments Regarding Further Notice of Proposed Rulemaking," CC Docket No. 97–213 at 77–81) and in their brief before the D.C. Circuit Court of Appeals (see Final Brief for the United States at 15–18).

With reference to the aforementioned FBI/DOJ Comments before the FCC, we note, as did the FBI/DOJ Comments at pages 79–80, that there is nothing in CALEA or its legislative history to indicate that Congress meant to prohibit the use of law enforcement electronic surveillance equipment which has the capability of separating signals of communications content from communications transactional information. For example, all "local loop" electronic surveillance efforts necessitate such tools and approaches. And no one, to our knowledge, is suggesting,for example, that "local loop" interceptions are in any way affected or curtailed by CALEA or otherwise. Further, to quote from the Comments:

"It is worth noting that Section 103(a)(4) does not state that carriers "shall no deliver" communications and call-identifying information that law enforcement is not authorized to intercept, but only that carriers shall "protect the privacy and security" of such information. A carrier is entitled to rely on enforcement's discharge of its legal obligation under 18 U.S.C. § 3121(c) as a means of "protecting the privacy" and security" of information that law enforcement is not authorized to intercept. Accordingly, the J-Standard is not deficient in this regard."

Comments at 80. Moreover, with reference to the aforementioned FBI/DOJ Brief, we quote the following:

"* * * because the use of minimizing technology under Section 3121(c) can prevent law enforcement agencies from hearing or seeing the content portion of a pack-

et stream, the J-Standard does not offend Title III or the Fourth Amendment. *Cf. United States* v. *Miller*, 116F.3d 641, 659–60 (2d Cir. 1997) (use of pen register device that is capable of recording call content as well as dialing information does not violate Title III), *Sanders* v. *Robert Bosch Corp.*, 38 F.3d 736, 742 (4th Cir. 1994) (no Title III interception occurred when oral conversations were monitored and transmitted by hidden microphone but contents of conversations were neither heard nor recorded)."

Brief at 17. Thus, in light of the above, and notwithstanding any concerns which may have been expressed by the court with regard to packet-switched communications generally, we believe, both with regard to networks of telecommunications carriers and the networks of computer-based "information services," that privacy and security protection can be satisfied in privacy-enhancing electronic surveillance tools such as Carnivore. Since we believe that privacy and security protection can be, and is being, maintained, we do not necessarily share the *rendition* of "privacy concerns" as alluded to in the dicta of the D.C. Court of Appeal's CALEA-based decision.

*Question 10.* The public concern about use of Carnivore and government surveillance of the Internet has prompted at least one witness at the hearing to call for more Congressional oversight. In this connection, I introduced last year as part of the E–RIGHTS Act, S. 854, a proposal to require the Attorney General to provide the Congress annual reports on the number of warrants, court orders and subpoenas for government interceptions of e-mail and other electronic communications under 18 U.S.C. section 2703. What is your view of whether this proposal would assist Congress in providing appropriate oversight and necessary information about government practices under the law?

Answer 10. The FBI is certainly on record as being amenable to Congressional oversight, including in the area of electronic surveillance. As noted in the last section of our Hearing statement for the record, a great deal of Congressional oversight already exists, particularly in the area of electronic surveillance. With regard to whether it is a good idea to require the Attorney General to provide to the Congress detailed annual reports regarding all of the Department of Justice agency components' warrants, court orders, and subpoenas pertaining to governmental acquisitions of stored E-mail and other electronic communications obtained under 18 U.S.C. § 2703, we would defer to the Department of Justice.

SENSITIVE INFORMATION NONDISCLOSURE AGREEMENT

An Agreement between _____ and the Federal Bureau of Investigation (FBI) regarding the nondisclosure of sensitive FBI information, to wit: any and all information received, observed, or otherwise required from the FBI or the U.S. Department of Justice (DOJ) arising from a review requested by the Attorney General of the United States (the Review) of the FBI's Carnivore device and system, including, but not limited to, any and all information pertaining to the Carnivore software and associated software and hardware devices and systems; any and all information pertaining to investigations, investigative uses, operations, procedures, policies, practices, guidelines, contracts, sensitive (including proprietary) governmental information, nongovernmental proprietary information, training, training documents, manuals, technical descriptions, source code, object code, executable software, designs and design information, documentation, descriptions, tests, test results, test scenarios, deficiencies, and vulnerabilities associated with the Carnivore device and system ("Sensitive Information").

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to Sensitive Information from the FBI or the DOJ arising from the Review as required to perform my duties. I also understand and accept that by being granted access to this Sensitive Information, special confidence and trust shall be placed in me by the FBI.

2. I hereby acknowledge that I have been briefed concerning the nature and protection of Sensitive Information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures. Further, I understand that unauthorized use or disclosure of Sensitive Information, marked or unmarked, including, but not limited to, oral communications or information observed or gleaned arising from the Review, may compromise, jeopardize or subvert current, past, or future law enforcement activities, investigations, or investigative techniques and may compromise, jeopardize or subvert existing or future FBI contracts, contractual relationships between the FBI and vendors, or the ability of the FBI to effectively contract with vendors now or in the future.

3. I agree to manage all Sensitive Information in a manner consistent with procedures recommended by the FBI or DOJ, and I will not now or in the future use,

disclose, or retain Sensitive Information unless such disclosure is necessary in the performance of the Review, and I have either officially verified that the recipient of such information has been properly authorized by the FBI or DOJ to receive it, or been given prior written notice of authorization from the FBI or the DOJ that such use, disclosure or retention is permitted. I understand that if I am uncertain as to the sensitive nature or status of information as Sensitive Information, I am required to confirm from an authorized FBI or DOJ official that such information may be used, disclosed or retained prior to its use, disclosure or retention. The obligations imposed upon me herein shall not apply to Sensitive Information which is disclosed pursuant to a valid order of a court or governmental body or any political subdivision thereof; provided, however, that I shall first have given notice to the FBI or DOJ in order to permit them to seek a protective order and in such case I shall assist the FBI or DOJ in filing a protective order in accordance with applicable rules; and if such order issues, disclosure under this provision shall be made only in accordance with the terms of the protective order. Not withstanding this provision, IITRI shall be able to retain one (1) copy of the draft and final reports provided to the FBI or DOJ as a result of the Review for a period of one year after completion of the Review, after which time such copies shall be returned to the FBI or DOJ.

4. I have been advised that except as necessary for the Review, any effort to reverse engineer the Carnivore software or other software, including software code, to which I may be given access during the Review may cause irreparable damage to (a) FBI investigations and investigative techniques; (b) FBI contracts, contracting capabilities, contractual relationships between the FBI and vendors, or the ability of the FBI to effectively contract with vendors now and in the future; or (c) the rights of third parties to protect their proprietary information; and I will not undertake any such action, use, or effort to reverse engineer Carnivore or other software, including software code, or undertake any other action, use, or effort that is inconsistent with the sensitive and protected nature of this software, unless I have been given prior and explicit written authorization from the FBI or DOJ that such action, use, or effort is permitted. I will also not duplicate or copy Sensitive Information arising from the Review in a manner inconsistent with the procedures recommended by the FBI or DOJ. I acknowledge that unauthorized duplication or copying of Sensitive Information arising from the Review may cause irreparable damage to FBI investigations, investigative techniques, or contracting capabilities.

5. I have been advised that any breach of this Agreement may result in the termination of my relationship with the FBI and the DOJ and my removal from the Review. In addition, I have been advised that any unauthorized disclosure, use, or retention of Sensitive Information by me may constitute a violation or violations of United States criminal laws, including those codified in title 18, United States code, or may lead to criminal prosecution for obstruction of lawful government functions. I realize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

6. I understand that all Sensitive Information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or in the control of the FBI or DOJ unless otherwise determined by an authorized FBI or DOJ official or final ruling in a court of law. I agree that I shall return all Sensitive Information provided to me by the FBI or DOJ in written or any other tangible form which has come or may come into my possession, or for which I am responsible because of such access: (a) upon demand by an authorized representative of the FBI or the DOJ, or (b) upon the conclusion of my relationship with the FBI or the DOJ incidental to this Review, whichever occurs first.

7. Unless and until I am released in writing by an authorized representative of the FBI or the DOJ, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to the Sensitive Information and at all times thereafter.

8. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

9. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure or use of Sensitive Information in breach of this Agreement. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, use, or retention of Sensitive Information not consistent with the terms of this Agreement.

10. I have read this Agreement carefully and my questions, if any, have been answered.

*Signature*_____ *Date*_____
Organization (if contractor, provide name and address):
The briefing and execution of this Agreement was witnessed by

*(type or print name)*

Signature_____ Date _____

Security Debriefing Acknowledgment

I reaffirm that the provisions of the Federal criminal laws applicable to the safeguarding of Sensitive Information have been made available to me by the FBI or DOJ; that I have returned all Sensitive Information in my custody; that I will not use, disclose or retain myself Sensitive Information to any unauthorized person or organization; that I will promptly report to the FBI any attempt by an unauthorized person to solicit Sensitive Information; and that I have received a debriefing regarding the security of Sensitive Information.

*Signature*_____ *Date* _____

*Name of Witness (type or print)*_____

*Signature of Witness*_____ *Date* _____

○