STATEMENT OF
KEVIN V. Di GREGORY
DEPUTY ASSISTANT ATTORNEY GENERAL
UNITED STATES DEPARTMENT OF JUSTICE
BEFORE THE SUBCOMMITTEE ON THE CONSTITUTION
OF THE HOUSE COMMITTEE ON THE JUDICIARY
on
"CARNIVORE" AND THE FOURTH AMENDMENT

July 24, 2000

Mr. Chairman and Members of the Subcommittee, thank you for allowing me this opportunity to testify about the law enforcement tool "Carnivore" and the Fourth Amendment. On April 6, 2000, I had the privilege of testifying before you during a hearing on Internet privacy and the Fourth Amendment. I am pleased to continue to participate in the discussion today about "Carnivore" and its role in protecting individual privacy on the Internet from unwarranted governmental intrusion, and about the critical role the Department plays to ensure that the Internet is a safe and secure place.

Privacy and Public Safety

It is beyond dispute that the Fourth Amendment protects the rights of Americans while they work and play on the Internet just as it does in the physical world. The goal is a long-honored and noble one: to preserve our privacy while protecting the safety of our citizens. Our founding fathers recognized that in order for our democratic society to remain safe and our liberty intact, law enforcement must have the ability to investigate, apprehend and prosecute people for criminal conduct. At the same time, however, our founding fathers held in disdain the government's disregard and abuse of privacy in England. The founders of this nation adopted the Fourth Amendment to address the tension that can at times arise between privacy and public

safety. Under the Fourth Amendment, the government must demonstrate probable cause before obtaining a warrant for a search, arrest, or other significant intrusion on privacy.

Congress and the courts have also recognized that lesser intrusions on privacy should be permitted under a less exacting threshold. The Electronic Communications Privacy Act ("ECPA") establishes a three-tier system by which the government can obtain 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, in order to obtain source and destination information in real time, the government must obtain a "trap and trace" or "pen register" court order authorizing the recording of such information. *See* 18 U.S.C. 1821 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 the Fourth Amendment requires. In the absence of a statutory exception, the government needs a court order to wiretap communications. To obtain such an order, the government must show that normal investigative techniques for obtaining the information have or are likely to fail or are too dangerous, and that any interception will be conducted so as to ensure that the intrusion is minimized.

The safeguards for privacy represented by the Fourth Amendment and statutory restrictions on government access to information do not prevent effective law enforcement. Instead, they provide boundaries for law enforcement, clarifying what is acceptable evidence

gathering and what is not. At the same time, those who care deeply about protecting individual privacy must also acknowledge that law enforcement has a critical role to play in preserving privacy. When law enforcement investigates, successfully apprehends and prosecutes a criminal who has stolen a citizen's personal information from a computer system, for example, law enforcement is undeniably working to protect privacy and deter further privacy violations. The same is true when law enforcement apprehends a hacker who compromised the financial records of a bank customer.

As we move into the 21st century, we must ensure that the needs of privacy and public safety remain in balance and are appropriately reflected in the new and emerging technologies that are changing the face of communications. 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. 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.

Law Enforcement Tools in Cyberspace:

Although the Fourth Amendment is over two centuries old, the Internet as we know it is still in its infancy. The huge advances in the past ten years have changed forever the landscape of society, not just in America, but worldwide. The Internet has resulted in new and exciting ways for people to communicate, transfer information, engage in commerce, and expand their educational opportunities. These are but a few of the wonderful benefits of this rapidly changing technology. As has been the case with every major technological advance in our history,

however, we are seeing individuals and groups use this technology to commit criminal acts. As Deputy Attorney General Eric Holder told the Crime Subcommittee of this Committee in February, our vulnerability to computer crime is astonishingly high and threatens not only our financial well-being and our privacy, but also this nation's critical infrastructure.

Many of the crimes that we confront everyday in the physical world are beginning to appear in the online world. Crimes like threats, extortion, fraud, identity theft, and child pornography are migrating to the Internet. 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 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 satisfy our obligations to the public to enforce the laws and preserve the 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, statutory, internal and court-ordered boundaries. Carnivore is simply an investigatory tool that is used online only under narrowly defined circumstances, and only when authorized by law, to meet our responsibilities to the public.

To illustrate, law enforcement often needs to find out from whom a drug dealer, for instance, is buying his illegal products, or to whom the drug dealer is selling. To investigate this, it is helpful to determine who is communicating with the drug dealer. In the "olden days" of perhaps 10 years ago, the drug dealer would have communicated with his supplier and customers exclusively through use of telephones and pagers. Law enforcement would obtain an order from a court authorizing the installation of a "trap and trace" and a "pen register" device on the drug dealer's phone or pager, 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 his phone calls would have been recorded. This is information that courts have held is not protected by 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 drug dealer may be just as likely to send an e-mail as call his confederates. When law enforcement uses a "trap and trace" or "pen register" in the online context, however, we have found that, at times, the Internet service provider has been unable or even unwilling to supply this information. 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. We cannot do this without tools like 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 (which does not include the content of the message) is often mixed in with a lot of other non-content data that we have no desire or authority 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 Carnivore. If, however, the service provider is unwilling or unable to comply with the order, we simply cannot give a criminal a free pass. It is for that narrow set of circumstances that the FBI designed "Carnivore."

Carnivore is, in essence, a special filtering tool that can gather the information authorized by court order, and only that information. It permits law enforcement, for example, to gather only the email addresses of those persons with whom the drug dealer 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. In other words, Carnivore is a *minimization* tool that permits law enforcement strictly to comply with court orders, strongly to protect privacy, and effectively to enforce the law to protect the public interest. In addition, Carnivore creates an audit trail that demonstrates exactly what it is capturing.

As with any other investigative tools, there are many mechanisms we have in place to prevent against possible misuse of Carnivore, and to remedy misuse that has occurred. The Fourth Amendment, of course, restricts what law enforcement can do with Carnivore, as do the statutory requirements of Title III and the Electronic Communications Privacy Act, and 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 wire or electronic communications, the requesting investigatory agency must obtain approval 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 the Fourth Amendment requirements, and is in compliance with applicable statutes and regulations. Similarly, typically the U.S. Attorney or the section chief within the Department who is handling the investigation also reviews the Title III intercept request. Even if the proposal clears the OEO, approval must be given by a Deputy Assistant Attorney General. 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 approved by the proper court. 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 investigatory 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 III 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.

Carnivore itself also contains self-regulating features. For example, because of its sophisticated passive filtering features, it automates the process of minimization without intrusive monitoring by investigators, and simply disregards packets of information that do not satisfy the criteria in the court's authorization. Indeed, one of the most powerful privacy-protecting features of Carnivore is its ability to ignore information that is outside the scope of the court-ordered authority. For later verification, it also logs the filter settings. In addition, as a practical matter, Carnivore is not deployed except with close cooperation with the appropriate system provider. In any event, the FBI does not use Carnivore in every instance in which the court orders a Title III electronic communication intercept. Indeed, I understand that the Bureau uses Carnivore only in those instances when the service provider is unable to comply with the court order using its own equipment, or when the provider asks the FBI to use Bureau equipment.

As I testified in April, we face three major categories of challenges in trying to keep the Internet a safe and secure place for our citizens. These are:

1. Technical challenges that hamper law enforcement's ability to locate and prosecute criminals that operate online;

2. Certain substantive and procedural laws that have not kept pace with the changing technology, creating significant legal challenges to effective investigation and prosecution of crime in cyberspace; and

3. Resource needs that must be addressed to ensure that law enforcement can keep pace with changing technology and has the ability to hire and train people to fight cybercrime.

Carnivore is an investigative tool that assists us in meeting the first challenge. As we have witnessed, tracking a criminal online is not always an impossible task using our investigative tools. For example, last year federal and state law enforcement combined to successfully apprehend the creator of the Melissa virus and the individual who created a fraudulent Bloomberg News Service website in order to artificially drive up the stock price of PairGain, a telecommunications company based in California. Although we are proud of these important successes, we still face significant challenges as online criminals become more and more sophisticated.

In nearly every online case, tracking the online criminal requires law enforcement to attempt to trace the "electronic trail" from the victim back to the perpetrator. In effect, this "electronic trail" is the fingerprint of the twenty-first century – only much harder to find and not

as permanent as its more traditional predecessor. In the physical world, a criminal and his victim are generally in the same location. But cybercriminals do not have to physically visit the crime scene. Instead they cloak their illegal activity by weaving communications through a series of anonymous remailers, by creating forged e-mail headers with powerful point and click tools readily downloadable from hacker websites, by using a "free-trial" account or two, or by "wiping clean" the logging records that would be evidence of their activity.

In some cases, the criminal may not even be in the same country as the victim. The global nature of the Internet, while one of the greatest assets of the Internet to law-abiding citizens, allows criminals to conduct their illegal activity from across the globe. In these cases, the need to respond quickly and track the criminal is increasingly complicated and often frustrated by the fact that the activity takes place throughout different countries. With more than 190 countries connected to the Internet, it is easy to understand the coordination challenges that face law enforcement. Furthermore, in these cases, time is of the essence and the victim may not even realize they have been victimized until the criminal has long since signed-off. Clearly, the technical challenges for law enforcement are real and profound.

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

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

2. We must recognize that the needs and challenges of law enforcement posed by the Internet are substantial, including our the need for resources, up-to date investigative tools and enhanced multi-jurisdictional cooperation.

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

I would encourage anyone with an interest in this important topic to review carefully the report of the Working Group. The report can be found on the Internet by visiting the website of the Department of Justice's Computer Crime and Intellectual Property Section, located at www.cybercrime.gov. In addition to the report, www.cybercrime.gov also contains other useful information on a wide array of Internet related issues, including the topic of today's hearing – privacy.

Despite the type of difficulties outlined in the Unlawful Conduct Report and discussed today, 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.

Mr. Chairman, the Department of Justice has taken 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. CCIPS was founded in 1991 as the Computer Crime Unit, and became a Section in 1996. CCIPS has grown from five attorneys in 1996 to twenty 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 infrastructures. 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, I want to thank you again for this opportunity to testify today about our efforts to fight crime on the Internet while preserving the rights conferred by the Fourth Amendment and statute. Ultimately, the decision as to the appropriate parameters of law enforcement activity lies squarely within the Constitution and the elected representatives of the people, the Congress. The need to protect the privacy of the American people -- not just from the government but also from criminals -- is a paramount consideration, not just in the context of the Internet, but in general. The Department of Justice stands ready to work with this Subcommittee and others to achieve the proper balance between the important need for protecting privacy and the need to respond to the growing threat of crime in cyberspace.

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

-original (since finished)

Statement for the Record of
Donald M. Kerr
Assistant Director
Federal Bureau of Investigation
Before the
United States House of Representatives
The Committee on the Judiciary
Subcommittee on the Constitution
Washington, D.C.
7/24/2000

Good afternoon, Mr. Chairman, and Members of the Subcommittee. I am grateful for this opportunity to discuss the FBI's Internet and data interception capabilities and to help set the record straight regarding this important issue. I would like to first discuss FBI's legal authority for conducting interceptions on the Internet, and then describe Carnivore and how we use it.

Two weeks ago, the Wall Street Journal published an article entitled "FBI's system to covertly search e-mail raises privacy, legal issues." This story was immediately followed by a number of similar reports in the press and other media depicting Carnivore as something ominous and raising concerns about the possibility of its potential to snoop, without a court order, into the private E-mails of American citizens. I think that it is important that this topic be discussed openly--and in fact this was the purpose behind the FBI choosing to share information regarding this capability with the industry experts several weeks ago. It is critically important that, as technology, and particularly communications technology, continues to evolve rapidly, the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. I believe that it is also very important that these discussions be placed into the context into which they properly belong and that the true facts concerning this issue are made clear. More to the point,

that these capabilities are used only with lawful authorization and that they are directed at the most egregious violations of national security and public safety

First of all, the FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived in part from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), which is commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". I want to stress that all such interceptions, with the exception of a rarely used "emergency" authority or consent of a participant in the communication, are performed under a court order issued by a judge. Under emergency provisions, the Attorney General, the Deputy or the Associate Attorney General may, if authorized, initiate electronic surveillance of wire or electronic communications without a court order, but only if an application for such order is made within 48 hours after the surveillance is initiated.

Federal surveillance laws must comply with the Fourth Amendment's dictates concerning reasonable searches and seizures, but they also include a number of provisions that are intended to ensure that this investigative technique is used judiciously and with deference to the privacy of intercepted subjects and certainly with deference to the privacy of those who are not the subject of the court order.

For example, unlike search warrants for physically searching a house, under Title III and Department of Justice policy, applications for interception of oral, wire and electronic

communications require the authorization of a high-level Department of Justice (DOJ) official before the local United States Attorneys offices can make an application to a federal court Further, interception of communications is limited to certain federal criminal offenses.

Applications for electronic surveillance must demonstrate probable cause and state with particularity and specificity: the offenses being committed, the telecommunications facility or place from 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. Thus, criminal electronic surveillance laws focus on gathering hard evidence - not intelligence.

Applications must indicate that other normal investigative techniques have been tried and failed to gather evidence of crime, or will not work, or are too dangerous, and must include information concerning any prior electronic surveillance regarding the subject or facility in question. Court orders are initially limited to 30 days, with extensions possible, and must terminate sooner if the objectives are obtained. Judges may, and usually do, require periodic reports to the court, typically every 7 to 10 days, advising it of the progress of the interception effort. This assures close and on-going oversight of the electronic surveillance by the United States Attorney's office handling the case and frequently the court.

Interceptions are required to be conducted in such a way as to "minimize the interception of communications not otherwise subject to interception" under the law, such as unrelated, irrelevant, and non-criminal communications of the subjects and of others not named in the application.

To ensure privacy protection and evidentiary integrity of the communications that are intercepted, such intercepted communications are required to be recorded, if possible, on tape or other device, and recorded in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings are then required to be presented to the federal district court judge and sealed under his or her directions. The presence of the seal shall be a prerequisite for their use or disclosure, or for the introduction of evidence derived from the tapes. Applications and orders signed by the judge are also to be sealed by the judge.

Within a reasonable period of time after the termination of the intercept order, including extensions, the judge shall ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, providing notice of the order, the dates during which the interceptions were carried out, and whether or not the person was intercepted. Upon motion, the judge may also direct that portions of the contents of the intercepted communication be made available to for their inspection.

Any person who was a party to an intercepted communication or was a party against whom an interception was directed may in any trial, hearing, or other proceeding move to suppress the con-

tents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was intercepted in violation of Title III, ECPA or the Fourth Amendment.

The illegal, unauthorized conduct of electronic surveillance is a federal criminal offense punishable by imprisonment for up to five years, a fine, or both. In addition, any person whose communications are unlawfully intercepted, disclosed, or used, may in a civil action recover from the person or entity engaged in the violation civil damages, including, if appropriate, punitive damages, as well as attorney's fees and other costs incurred.

The technical assistance of the service providers in helping a law enforcement agency execute an electronic surveillance order is always important, and in many cases it is absolutely essential. This circumstance is increasingly the case with the advent of advanced communications services and networks such as the Internet. Title III mandates service provider assistance incidental to law enforcement's execution of electronic surveillance orders by specifying that a court order authorizing the interception of communications shall upon the request of the applicant, direct that a "service provider, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted."

In practice, judges may sign two orders: one order authorizing the law enforcement agency to conduct the electronic surveillance, and a second, abbreviated, assistance order directed to the service provider, specifying, for example in the case of E-mail, the E-mail account name of the subject that is the object of the order and directing the provision of necessary assistance.

Service providers and their personnel are subject to the electronic surveillance laws like public officials and private persons. That is, unauthorized electronic surveillance is forbidden, and criminal and civil liability may be assessed for violations. Not only are unauthorized interceptions proscribed, but so also is the use or disclosure of the contents of communications that have been illegally intercepted. It is for this reason, among others, that service providers typically take great care in providing assistance to law enforcement in carrying out electronic surveillance pursuant to court order. In some instances, service providers opt to provide "full" service, essentially carrying out the interception for law enforcement and providing the final interception product, but, in most cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception. I want to stress that the FBI does not conduct interceptions, install and operate pen registers, or use trap & trace devices without lawful authorization from a court.

In recent years, it has become increasingly common for the FBI to seek, and for judges to issue, orders for Title III interceptions which are much more detailed than older orders which were directed against "plain old telephone services." These detailed orders, in order to be successfully implemented, require complex approaches to ensure that only messages for which there is

probable cause to intercept are, in fact, intercepted. The fact that court orders are becoming more detailed is in response, I think, to two facts.

First, the complexity of modern communications networks, like the Internet, as well as the complexity of modern users' communications demand better discrimination than for older analog communications. For example, Internet users frequently use electronic messaging services, like E-mail, to communicate with other individuals in a manner reminiscent of a telephone call, only with text instead of voice. Such messages are often the targets of court ordered interception. Users also use services, like the world wide web, which looks more like print media than a phone call Similarly, some Internet services, like streaming video, have more in common with broadcast media like television, than with telephone calls. These types of communications are less commonly the targets of an interception order

The second fact is that for many Internet services, users share communications channels, addresses, etc. These facts make the interception of messages for which law enforcement has probable cause, to the exclusion of all others, very difficult. Court orders are therefore increasingly written to include detailed instructions for ensuring that the privacy of communications for which there is no probable cause to intercept is guaranteed.

In response to a critical need for tools to implement these complex court orders, the FBI developed a number of capabilities including the software program called "Carnivore." Carnivore is a very specialized network analyzer or "sniffer" which runs on a normal Personal Computer running the

Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user. If the device is placed at some point on the network where it cannot discriminate messages as set out in the court order, it simply lets all such messages pass by unrecorded.

One might ask, "why use Carnivore at all?" In many instances, ISPs, particularly the larger ones, maintain capabilities which allow them to comply, or partially comply with lawful orders. For example, many ISPs have the capability to "clone" or intercept, when lawfully ordered to do so, E-mail to and from specified user accounts. In such cases, these abilities are satisfactory and allow full compliance with a court order. However, in most cases, ISPs do not have such capabilities or cannot employ them in a secure manner. Also, most systems devised by service providers or purchased "off the shelf" lack the ability to properly discriminate between messages in a fashion

that complies with the court order. Also, many court orders go beyond E-mail, specifying other protocols to be intercepted such as instant messaging. In these cases, a cloned mailbox is not sufficient to comply with the order of the court.

Now, I think it is important that you understand how Carnivore is used in practice. First, there is the issue of scale. Carnivore is a small-scale device intended for use only when and where it is needed. In fact, each Carnivore device is maintained at the FBI Laboratory in Quantico until it is actually needed in an active case. It is then deployed to satisfy the needs of a single case or court order, and afterwards, upon expiration of the order, the device is removed and returned to Quantico

The second issue is one of network interference. Carnivore is safe to operate on IP networks. It is connected by a high impedance bridge and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that the Carnivore is satisfactorily isolated from the network to which it is attached. Also, Carnivore is only attached to the network after consultation with, and with the agreement of, technical personnel from the ISP.

This, in fact raises the third issue--that of ISP cooperation. To date, Carnivore has, to my knowledge, never been installed onto an ISP's network without assistance from the ISP's technical personnel. The Internet is a highly complex and heterogeneous environment in which to conduct such operations, 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

successfully implement, and comply with the strict language, of an interception order. The FBI also depends upon the ISP personnel to understand the protocols and architecture of their particular networks.

Another primary consideration for using Carnivore is data integrity. As you know, Rule 901 of the Federal Rules of Evidence require the authentication of evidence as a precondition for its admissibility. The use of the Carnivore system by the FBI to intercept and store communications provides for an undisturbed chain of custody by providing a witness who can testify to the retrieval of the evidence and the process by which it was recorded. Performance is also a key reason for the use of Carnivore over commercial sniffers. Unlike commercial software sniffers, Carnivore is designed to intercept and record the selected communications comprehensively, without "dropped packets."

In conclusion, I would like to say that over the last five years or more, we have witnessed a continuing, steady growth in instances of computer-related crimes, including traditional crimes and terrorist activities which have been planned or carried out, in part, using the Internet. The ability of the law enforcement community to effectively investigate and prevent these crimes is, in part, dependant upon our ability to lawfully collect vital evidence of wrongdoing. As the Internet becomes more complex, so do the challenges placed on us to keep pace. We could not do so without the continued cooperation of our industry partners and innovations such as the Carnivore software.