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 Internet and data interception capabilities developed by the Federal Bureau of Investigation. The use of computers and the Internet is growing rapidly, paralleled by exploitation of computers, networks, and data bases to commit crimes and to harm the safety, security, and privacy of others. Criminals use computers to send child pornography to each other using anonymous, encrypted communications; hackers break into financial service companies systems and steal customer home addresses and credit card information; criminals use the Internet's inexpensive and easy communications to commit large scale fraud on victims all over the world; and terrorist bombers plan their strikes using the Internet. Investigating and deterring such wrongdoing requires tools and techniques designed to work with new evolving computers and network technologies. The systems employed must strike a reasonable balance between competing interests - the privacy interests of telecommunications users, the business interest of service providers, and the duty of government investigators to protect public safety. I would like to discuss how the FBI is meeting this challenge in the area of electronic mail interception.

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 our Carnivore system 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 reason we choose to share information about this capability with industry experts several weeks ago. It is critically important as technology, and particularly communications technology, a continues to evolve rapidly, that the public be guaranteed that their government is observing the statutory and constitutional protections which they demand. It is also very important that these discussions be placed into their proper context and that the relevant facts concerning this issue are made clear. I welcome this opportunity to stress that our intercept capabilities are used only after court approval and that they are directed at the most egregious violations of national security and public safety.

The FBI performs interceptions of criminal wire and electronic communications, including Internet communications, under authorities derived from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended), commonly referred to as "Title III", and portions of the Electronic Communications Privacy Act of 1986 (as amended), or "ECPA". Such federal government interceptions, with the exception of a rarely used "emergency" authority or in cases involving the consent of a participant in the communication, are conducted pursuant to court orders. 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 apply the Fourth Amendment's dictates concerning reasonable searches and seizures , and include a number of additional provisions which ensure that this investigative technique is used judiciously, with deference to the privacy of intercepted subjects and 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, applications for interception of wire and electronic communications require the authorization of a high-level Department of Justice (DOJ) official before the local United State Attorneys offices can make an application to a federal court. Unlike typical search warrants, federal magistrates are not authorized to approve such applications and orders, instead, the applications are veiwed by federal district court judges. Further, interception of communications is limited to certain specified federal felony 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 type 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 met. 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 by the court as well. 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 or others not named in the application.

To ensure the evidentiary integrity of intercepted communications they must be recorded, if possible, on magnetic tape or other devices, so as to protect the recording from editing or other alterations. Immediately upon the expiration of the interception period, these recordings must be presented to the federal district court judge and sealed under his or her directions. The presence of the seal is 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 extension, the judge is obligated by law to ensure that the subject of the interception order, and other parties as are deemed appropriate, are furnished an inventory, that includes notice of the order the dates

during which the interceptions were carried out, and whetehr or not the communication were intercepted. Upon motion, the jusge may also direct that portion of the contents of the intercepted communication be made available to affected person for their inspection.

Under Title III, any person who was a part 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 contents of any intercepted communication or any evidence derived therefrom if there are grounds demonstrating that the communication was not lawfully intercepted, the order authorizing or approving the interception was insufficient on its face or the interception was not in conformance with the order.

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 recover in a civil action damages, including punitive damages, as well as attorney's fees and other costs against the person or entity engaged in the violation.

The technical assistance of 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 is increasingly the case with the advent of advanced communication 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 communication shall upon the request of the applicant, direct that a telecommunications "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 also subject to the electronic surveillance laws, meaning that unauthorized electronic surveillance of their customers (or anyone else) 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 many cases, service providers are inclined only to provide the level of assistance necessary to allow the law enforcement agency to conduct the interception.

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 order, in order to be successfully implemented, require more sophisticated techniques to ensure that only messages for which there is court authorization to intercept are, in fact, intercepted. The increased detail in court orders responds to two facts.

First, the complexity of modern communications networks, like the Internet, and the complexity of modern users' communications demand better discrimination than 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.

Second, for many Internet services, users share communications channels, addresses, etc. These factors make the interception of messages for which law enforcement has court authorization, to the exclusion of all others, very difficult. Court orders, therefore, increasingly include detailed instructions to preclude the interception of communications that lie outside the scope of the order.

In response to a critical need for tools to implement 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 as an application program on a normal personal computer under 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 programmed 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 as a passive collection device and does not have any ability to transmit anything onto the network. In fact, we go to great lengths to ensure that our system 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 the Carnivore system is data integrity. As you know, Rule 901 of the Federal Rules of Evidence requires that 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 another key reason for preferring this system to 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, dependent 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. 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.

I look forward to working with the Subcommittee 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.