U.S. Department of Justice
Executive Office for United States Attorneys
United States Attorneys' USA Bulletin
March 2001 Vol. 49, No.2

Recognizing and Meeting Title III Concerns in Computer Investigations

Robert Strang

USA Bulletin

(March 2001)

Robert Strang
Assistant United States Attorney
Southern District of New York

The dramatic increase in crimes involving the Internet, and computer crimes more generally, is well documented. The "2000 CSI/FBI Computer Crime and Security Survey" documented that 90% of the 643 respondents (primarily large U.S. corporations and government agencies) detected computer security breaches within the last twelve months, totaling hundreds of millions of dollars in losses. In light of the increased criminal opportunities created by the ever-growing reliance on, and growing interconnectedness between network computers, there can be no doubt that experienced and sophisticated computer criminals pose a substantial challenge to law enforcement.

There has also been a corresponding increase in the difficulty in catching computer criminals. There are a number of reasons why this is so. The anonymity provided by computer communications has long been recognized as one of the major attractions to would-be computer criminal subjects. This difficulty has been heightened by the use and availability of so-called "anonymizers", services that repackage electronic mail and thereby diminish the ability to trace it. In addition, many victims and Internet Service Providers (ISPs) fail to record, or preserve for a sufficient length of time, historical logs and other records that might otherwise lead to the identification of subjects engaged in wrongdoing. Furthermore, the practice of jumping from compromised network to compromised network, including networks with servers located outside of the United States, can also make tracing the communications back to the initial subject extremely difficult. This is especially true where subjects have made efforts to cover their tracks or where proof of criminal activity, or even their fleeting presence, is lost before it can be secured. Finally, victims may be unaware of criminal activity on their network or, if aware, slow or unwilling to report it due to competitive reasons. For these and other reasons, there are many computer crimes where it will be impossible for law enforcement to identify the perpetrators involved. Therefore, exclusive reliance on historical investigations will allow criminal activity carried out by more experienced and skillful criminals to go undetected and/or unpunished.

Issues Raised by Proactive Investigations

As a result of these limitations, law enforcement is increasingly turning to proactive investigations where undercover agents seek out the individuals who are already engaging in computer crimes — attempting to record, in real-time, computer criminals while they are involved in the criminal act. The proactive approach bypasses some of the investigatory hurdles of anonymity, lack of records, and under-reporting inherent in computer cases. It also has the added benefit of potentially stopping the criminal before the damage is done. Use of real-time monitoring of criminal activity is even advantageous in some historical investigations where a subject returns to, or passes through the same victim's network. As criminals are increasingly adept at avoiding leaving an historic trail, such investigations are the next logical step for law enforcement (and one that is increasingly being taken).

Such undercover operations and recording are also feasible. The very expectation of anonymity that benefits criminals also helps law enforcement undercover agents enter this world without being scrutinized, as long as they can talk the talk. Agents can even use other undercover identities to vouch for themselves. From a technical perspective, so-called "sniffer" computer programs that are capable of recording all keystroke activity on a particular computer network are a well-known and widely available tool for system administrators, hackers, and law enforcement alike.

These types of investigatory techniques often raise legal issues. One of the major issues raised by real-time monitoring is compliance with federal wiretapping statutes. This article focuses on the ability to legally and contemporaneously record and identify subjects, and to develop admissible evidence which is central to a successful investigation. Agents and other investigators, some with only limited experience in this area may turn to prosecutors with questions regarding what they can and cannot do in their efforts to use real-time monitoring of criminals during the course of undercover operations. It is critical for prosecutors to be able to identify potential legal issues relating to such recordings by agents, in advance, before problems arise.

Since the current legal road map is largely without judicial markers, it is important to address some of the potential issues raised by the application of the privacy laws to real-time monitoring, as well as some of the statutory exceptions that may permit monitoring to take place absent a court order.

Application of Title III to "Electronic Communications"

In 1986, Congress passed the Electronic Communications Privacy Act ("ECPA"), which, among others things, extended the prohibitions contained in Title III of the Omnibus Crime and Control and Safe Streets Act of 1968 (the "Wiretap Act"), 18 U.S.C. §§ 2510-2521, to electronic communications that are intercepted contemporaneously with their transmission—that is electronic communications that are in transit between machines and which contain no aural (human voice) component. Thus, communications involving computers, faxes, and pagers (other than "tone-only" pagers) all enjoy the broad protections provided by Title III *unless* one or more of the statutory exceptions to Title III applies. In the computer context, both the government and

third parties are prohibited from installing "sniffer" computer software, such as the FBI's Carnivore program, to record keystroke and computer traffic of a specific target unless one of the exceptions is present.

Where the government is seeking to intercept and monitor all electronic communications originating from a target's home or through the e-mail account at the target's ISP, the application of Title III differs little from its historical application to telephone wiretaps. The issues agents and prosecutors are likely to encounter are typically technical, not legal. This is particularly true when law enforcement is dealing with ISPs who may have little or no experience in providing Title III assistance to law enforcement, have technical or manpower difficulties in providing access to the subject's accounts, or show an overall reluctance in working with law enforcement.

Sometimes, however, the potential effect of Title III's restrictions on computer law enforcement can be unexpected. For example, if a hacker breaks into a victim's computer, engages in criminal activity, and uses it to store credit card numbers, common sense would suggest the subject hacker enjoys no reasonable expectation of privacy. Perversely, however, the subject hacker's communications may enjoy statutory protection under Title III, and thus any interception of that illegal activity by a private party (including the victim) or law enforcement must fall within one of the statutory exceptions in order to monitor without a court order. In the above example, the victim's consent is likely to be sufficient to fall within one of Title III's statutory exceptions.

This example, however, becomes more difficult if the subject hacker simply uses the victim's computer as a jump point from which to illegally hop to new downstream victims or to communicate with the hacker's confederates, as is frequently the case. Does a victim have a right to monitor communications that are being made by a subject hacker who is trespassing on their computer, and is no longer seeking to damage it, but rather is passing through on his or her way to commit more mischief? Does the government enjoy the same rights to monitor that communication as the victim? How, if at all, does the analysis change when the government is the primary victim of the hacking activity?

The analysis of these scenarios is currently dependent on how courts interpret the breadth of existing statutory exceptions to Title III that were written to address the interception of simple, two-way telephone conversations. Thus, under current law, a hacker, a trespasser on another party's computer network, an intruder who enjoys no expectation of privacy, may nevertheless receive certain statutory protections under Title III. Prosecutors must therefore consider whether the statutory exceptions to Title III permit any proposed monitoring. The following are three statutory exceptions that appear to offer potential alternatives to the administrative and judicial burdens involved in seeking court-ordered monitoring under Title III.

Consent of a Party "Acting Under Color of Law"

The most commonly used exception to Title III's requirements permits "a person acting under color of law" to intercept an "electronic communication" where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c).

While there are not many judicial decisions in this area, two circuits appear to recognize that the owner of a computer may be considered a "party to the communication" and thus can consent to the government monitoring electronic communications between that computer and a hacker. *See United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993); *United States v. Seidlitz*, 589 F.2d 152, 158 (4th Cir. 1978). Thus, this exception appears to permit a victim to monitor and to authorize the government to monitor, hacking activity directly with his or her computer.

By contrast, if the communication merely passes through a victim's computer, a court may consider it a strain to conclude that the victim computer is a "party" to the communication. Technically, the victim's computer is receiving electronic communications and passing them on to downstream victims and/or confederates of the subject hacker. The literal possibility of monitoring this downstream traffic is present, as all the data streams through the victim's computer, but is the victim a "party to the communication" if the communications are simply passing through its system? A court may conclude that the owner is not a "party" capable of giving consent to key stroke monitoring given its pass through role.

This is more than a metaphysical concern. Hackers regularly seek to pass through the computers of victims they have previously hacked to: (1) cover their trail when they arrive at their next victim or victims; (2) continue to make use of favorable features of a compromised network such as storage space, bandwidth, and processing speed; (3) return to hacking tools they have left there for safekeeping; or (4) simply as a pattern of passing through old conquests to make sure their previous exploits have not been detected. This situation can arise even when a government computer is the initial victim. From there, the subject may hop (typically telnet) to the next network without taking the trouble of backing out of the hacked system. It is possible that the downstream network may not even be a true victim, but rather may belong to a system friendly to the subject hacker. In any event, the statutory exception requires that this new victim give "prior consent" to the monitoring, which will be almost an impossibility in the short term where the victim or victims typically cannot be known in advance.

Consent of a Party "Not Acting Under Color of Law"

Title III also permits "a person not acting under color of law" to intercept an "electronic communication" where "such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d).

In addition to permitting a victim to monitor communications to which he or she is a party before law enforcement gets involved, this exception provides a very powerful tool to law enforcement: obtaining the implied consent of the subject hacker himself or herself through computer "banners."

Computer networks frequently make use of computer banners that appear whenever a person logs onto the network. Each of us, for example, passes through such a banner each day when we log onto the Department of Justice's computer network. A banner is nothing more than a program that is installed to appear whenever a user attempts to enter a network from a designated point of entry known as a "port." Banners vary substantially in wording, but they usually inform the user that: (1) the user is on a private network; and (2) by proceeding, the user is consenting to

all forms of monitoring. Government networks already employ such broad-based banners, and we encourage private industry to follow suit. Businesses are often amenable to doing so, although often for non-law enforcement purposes, such as the monitoring of their employees' use of the Internet.

Thus, the subject hacker gives implied consent to monitoring whenever he or she passes through a properly worded banner. A properly worded banner should also result in implied consent by the subject hacker to the monitoring of all downstream activities, thus alleviating Title III concerns in much the same way as telephone monitoring of inmates, based on implied consent, has been upheld by the courts.

Due to their pervasiveness, the presence of banners is unlikely to deter or arouse suspicion in a subject who has already decided to enter a network illegally. In the case where a private network failed to have a sufficiently broad banner to permit monitoring, a later attempt to add a banner between visits may cause suspicion on the part of the hacker. Even in this situation, however, the very nature of the hacking experience frequently involves the constant cat and mouse game between network system administrators, seeking to remove hackers from their systems by terminating a compromised account and/or by "patching" the vulnerability that permitted the hackers to illegally enter the network, and the hackers attempting to return to the system and overcome and disable its security features. Thus, the addition of a new banner may not concern a dedicated hacker. The subject hacker may not be aware that Title III may prevent law enforcement from monitoring all of the intruder's activities while he or she is connected to the compromised computer network.

Finally, there are technical limitations to the use of banners. Computer systems are designed to have hundreds of ports for different types of uses such as electronic mail, remote log-in, or telnet. Most of these ports are not in use and remain closed, and can only be opened by a system administrator, or by a hacker who has illegally obtained the same privileges as a system administrator. Due to the technical nature of these ports, which goes beyond the scope of this article, it is not possible to install a banner or other message on a certain percentage of the ports. It is possible for a determined hacker to gain the same privileges (known as "superuser" or "root" status) on a network and open one or more of these ports, perhaps to serve as a future "back door" means of entry. Having once been given notice that the subject has given implied consent to monitoring by making use of a network, however, that consent should be valid for future use whether entry was made through a bannered or a non-bannered port. The only question this possibility raises is whether an affiliated or unaffiliated hacker might use one of these non-bannered ports for entry, and never pass through a banner.

Protection of the Rights and Property of the Provider

Title III also permits providers of a communication service, including an electronic communication service, the right to intercept communications as a "necessary incident to the rendition of his service" or to protect "the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i).

This exception permits a private party to monitor activities on its system to prevent misuse of the

system through damage, fraud, or theft of services. Since computer hacking often involves damage or disabling of a network's computer security system, as well as theft of the network's service, this exception permits a system administrator to monitor the activities of a hacker while on the network.

This exception to Title III has some significant limitations. One important limitation is that the monitoring must be reasonably connected to the protection of the provider's service, and not as a pretext to engage in unrelated monitoring. While no court has explored what this limitation means in the computer context, by way of analogy, one court has held that a telephone company may not monitor all the conversations of a user of an illegal clone phone unrelated to the protection of its service. *See McClelland v. McGrath*, 31 F. Supp.2d 616 (N.D. Ill. 1998).

Furthermore, the right to monitor is justified by the right to protect one's own system from harm. An ISP, for example, may not be able to monitor the activities of one of its customers under this exception for allegedly engaging in hacking activities on other networks. This limitation also makes it harder for a network administrator to justify the monitoring of hacking activities of a subject who has jumped to a new downstream victim. This potential limitation is unfortunate as it becomes more applicable precisely when the consent of a "party to the communication" is also at its weakest.

Another important limitation of this exception is that it does not permit a private provider of the communication service to authorize the government to conduct the monitoring; the monitoring must be done by the provider itself. Thus, where a provider lacks the technical or financial resources, or desire to engage in monitoring itself, it may be difficult for the government to step in to assist. Similarly, in situations where the government becomes aware that an ISP or network system administrator is monitoring illegal activity in order to protect its "rights and property," the government should be careful not to direct or participate in the monitoring, or cause it to be continued, because the provider may be deemed an agent of the government, and the exception may not apply. *Compare United States v. Pervaz*, 118 F.3d 1 (1st Cir. 1997), with *McClelland, infra*.

Even with these limitations, the provider exception can be very useful, particularly when a system administrator aggressively chooses to investigate hacking activity, or when the victim computer network is owned by the government. The technical gap in the use of implied consent described above, the inability to place consent banners on certain ports, can be filled by the use of the provider exception to monitor computer intrusions coming through these ports.

Conclusion

While Title III concerns are only one of the potential issues raised by proactive investigations in the computer context (others may include entrapment or even third-party liability), they are certainly among the most important. When all else fails, the prosecutor can always seek a Title III interception order. While this requires both departmental and judicial approval, there are a few aspects of obtaining such a "datatap" order that may make it less of a burden than obtaining a traditional telephone wiretap order. First, with respect to the interception of electronic communications, law enforcement is not limitedto predicate offenses, but rather may seek it for

any federal felony (note that some forms of hacking may constitute only a misdemeanor). *See* 18 U.S.C. § 2516(3). Second, with respect to the recording on or through a victim computer, the actual hacking activities typically constitute a federal felony, thus meeting the probable cause standards for seeking the authorization will be simple. *See* 18 U.S.C. § 2518(3)(a).

Third, the method of recording the results of the datatap are not difficult; the information can be obtained using specialized software or commercially available sniffer programs. Finally, minimization presents far less of a problem than it does for the execution of a traditional wiretap. *See* 18 U.S.C. § 2518(5). The burdens encountered and time lost in seeking Title III authorization makes the proper use of the exceptions discussed in this article extremely useful tools in investigating criminal activity. With the aid of proper monitoring, as well as the use of the many tools to obtain historical activities of subject hackers, law enforcement can overcome the potential anonymity provided by a computer, and identify and prosecute those criminals who abuse it to violate the law.

For more information on how Title III applies to the Internet, see Chapter 4 of the Computer Crime and Intellectual Property Section's new manual "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Criminal Investigations. It is available at www.cybercrime.gov/searchmanual.htm"

ABOUT THE AUTHOR

Robert Strang has been an Assistant UnitedStates Attorney for the Southern District of New York since 1997, where he currently serves as Computer Telecommunications Coordinator.

###