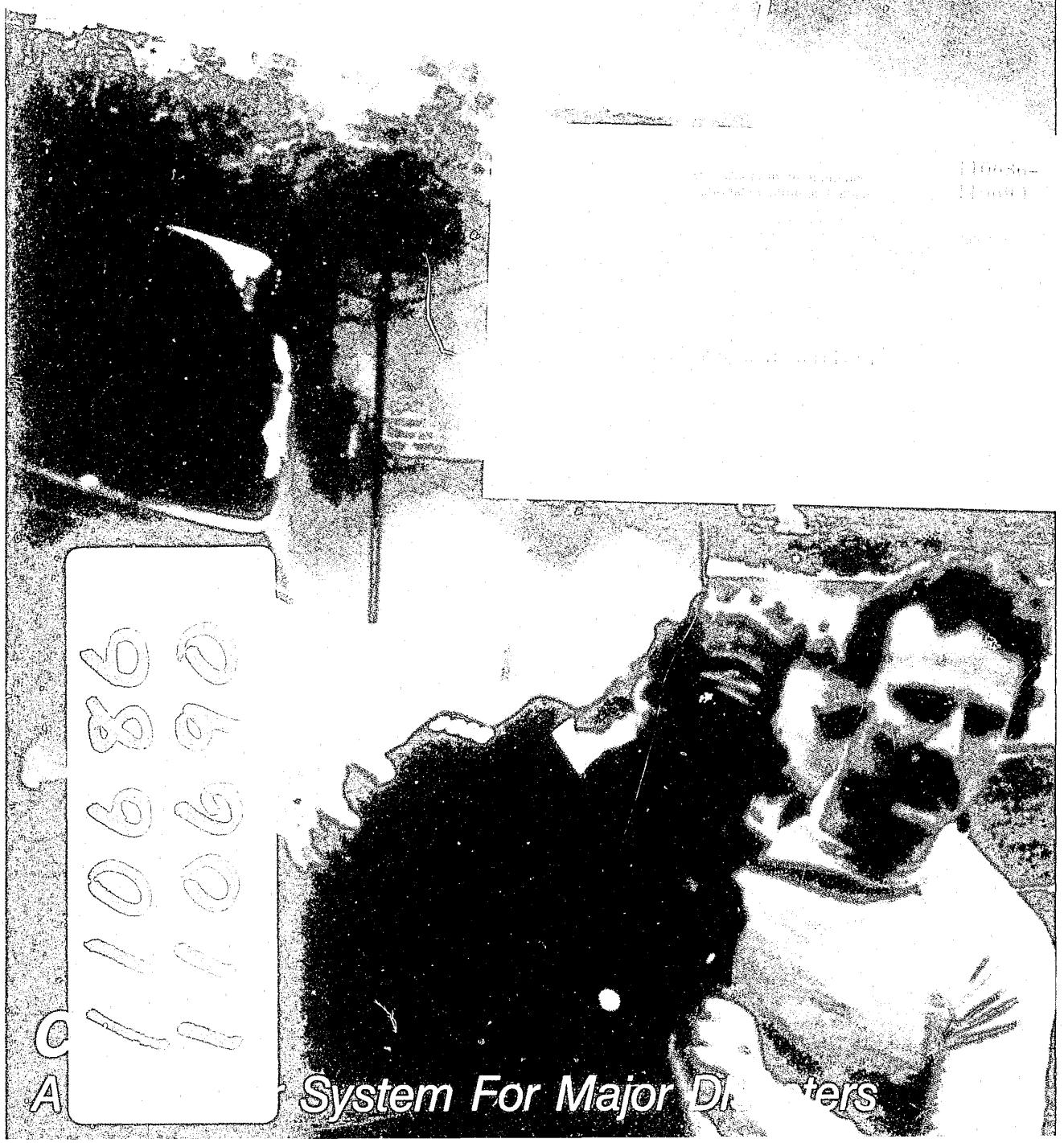
FBI

April 1988



A System For Major Di ters

Contents

April 1988, Volume 57, Number 4

FBI

Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William S. Sessions, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs,
Milt Ahlerich, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—John E. Ott
Production Manager/Reprints—*David C. Maynard*

The Cover:

The May 11, 1985, fire disaster at England's Bradford City football ground prompted the creation of the CRISIS computer system. (See article p. 8).

The FBI Law Enforcement Bulletin (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Ave., N.W., Washington, DC 20535. Second-Class postage paid at Washington, DC. Postmaster: Send address changes to Federal Bureau of Investigation, FBI Law Enforcement Bulletin, Washington, DC 20535.

ISSN 0014-5688 USPS 383-310

Director's Message

May 1988, is the 27th anniversary of President John F. Kennedy's approval of the law designating May 15 as Peace Officers Memorial Day. The words at Gettysburg of another eloquent, and assassinated, President are appropriate to honor "those who gave their lives that this nation might live."

President Kennedy's predecessor, Dwight D. Eisenhower, had established May 1 as Law Day 3 years before. While the theme of the 1988 Law Day is "legal literacy," one of the purposes of Law Day is to recognize the "support. . . [of] those. . . persons charged with law enforcement." In the decade 1977 to 1986, the FBI's Uniform Crime Reporting system has recorded 875 law enforcement officers feloniously killed. While law enforcement has reduced the 1979 high of 106 officers killed to a new low of 66 officers killed in 1986, this is still an unacceptable number, both in terms of the human tragedy involved and in sheer economics.

It is the duty, and the even greater moral obligation, of every law enforcement chief executive to see that the officers in his or her command have the very best training and equipment available to protect themselves in potentially deadly situations. Two of my predecessors, William H. Webster and Clarence M. Kelley, recognized and advocated the use of ballistic vests and training in night use of firearms. "The decline in officers killed is partially a result of technology, the development of Kevlar, the ballistic fiber used in soft body armor," according to FBI Director Webster, writing in this journal. Ten years before, Director Kelley pointed out that nighttime "and dimly lit situations predominate the encounters that prove fatal to law enforcement personnel." For this reason, the FBI then placed greater emphasis on training for these potentially dangerous nighttime encounters.

The loss of 875 officers in a decade is, and should be, sobering to every citizen. This represents more peace officers than all but the largest communities in this country have on their rolls—it is just under the size of the largest police department in Virginia, for example.

The man who led the FBI's efforts to successfully end the gangster era's bloody reign of terrror, J. Edgar Hoover, noted in one of the first Law Day messages, "The effectiveness of law is measured by the fairness, determination, and courage with which it is enforced. . . .Our society demands of the peace officer spotless integrity, uncommon bravery, and constant devotion to duty. It is fitting that Americans pause during the year to acknowledge a debt of gratitude to those who have been faithful to their trust."

It is also fitting that the law enforcement community, represented by 15 law enforcement organizations ranging from the International Association of Chiefs of Police and the National Sheriffs' Association to the Fraternal Order of Police and the National Organization of Black Law Enforcement Executives, has organized the National Law Enforcement Officers Memorial Fund to build a memorial to the thousands of officers who have given their lives to protect their fellow citizens since our Nation began.

I wholeheartedly support this memorial. As I said at the recent dedication of the FBI's Hall of Honor for fallen Special Agents, ". . .they could have chosen professions that paid far more, demanded much less, and presented few dangers. Instead they *chose* to carry the badge . . . and accepted the responsibility to do their duty." The same words of tribute apply to every peace officer in this land of ours built on the rule of law.

William S. Sessions

William S. Sessions
Director

110690

The Electronic Communications Privacy Act:
Addressing Today's Technology
(Conclusion)

By
ROBERT A. FIATAL, J.D.
Special Agent
Legal Counsel Division
FBI Academy
Quantico, VA

Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

Part one of this article identified the problem areas which caused Congress to pass the Electronic Communications Privacy Act[42] (the ECPA). Part two discussed the portion of the ECPA which requires law enforcement officers to obtain wiretap-type court orders to nonconsensually intercept electronic communications, to include messages sent to digital display pagers, messages sent from one computer terminal to another, and written messages, photographs, drawings, or documents electronically transmitted from one point to another.

Part three will now examine two remaining provisions of the ECPA of common significance to Federal, State, and local law enforcement officers. First, it will consider the required procedures to use pen registers and trap and trace devices. Second, it will address the required procedures to obtain stored electronic communications and transactional records of communications services.

Pen Registers and Trap and Trace Devices

The pen register device, which records the telephone numbers dialed from the phone targeted by the device, is a particularly useful investigative technique. It is of particular value in narcotics distribution investigations, providing the investigator a pattern of calls between suspected sources of supply, dealers, buyers, and money launderers. A trap and trace device, which determines the phone number from which a call is made, is invaluable in kidnapping and extortion investigations to determine the origin of ransom or extortionate calls. As discussed in part two of this article, the ECPA specifically states that law enforcement officers are not required to obtain wiretap-type orders to use these devices.[43]

Further, the Supreme Court has determined that the user of a telephone has no reasonable expectation of privacy in the numbers dialed from that phone.[44] The user could reasonably expect the telephone company to routinely use a pen register device for numerous legitimate purposes. Similarly, when one dials a number on the telephone, he voluntarily provides the telephone company the number of the phone he is dialing and assumes the risk that the telephone company might

Special Agent Fiatal

trace that call and provide the police with the number and location of the phone from which the call originated.[45] Therefore, law enforcement officers do not need to obtain a search warrant to use a pen register or trap and trace device, as those devices do not intrude into a reasonable expectation of privacy.

Nonetheless, phone companies, which provide necessary technical assistance to law enforcement when using pen registers and trap and trace devices, commonly insist in nonemergency situations upon some type of court authorization before providing their assistance. In order to set forth a standardized procedure for law enforcement officers to obtain court authorization for the use of pen registers and trap and trace devices and to provide limited judicial monitoring of the use of these devices by law enforcement, Congress, in the ECPA, set forth specific procedures that police officers must follow to obtain authorization for using these investigative techniques.

Although law enforcement officers are not required to obtain a traditional wiretap order or a search warrant to use pen registers or trap and trace devices, they must follow this proscribed procedure.[46] Federal officers have had to comply with this procedure since the ECPA's effective date of January 20, 1987. State and local law enforcement officers do not have to follow this procedure until 2 years after the effective date the act was passed, or by October 2, 1988, unless, of course, their respective State law is now more restrictive than the ECPA or their State adopts the ECPA's procedure prior to October 2, 1988.[47] For example, if State law requires a State law enforcement officer to obtain a search warrant to use a pen register device, officers in that State must continue to follow the State-mandated procedure.

Under the provisions of the ECPA, an attorney of the government, to include assistant U.S. attorneys and State and local prosecuting attorneys, or a State law enforcement officer must make written application, under oath, to a court of general criminal jurisdiction for proper authorization to use either a pen register or a trap and trace device.[48] Magistrates of U.S. district courts also have the power to approve these applications in Federal investigations.[49]

In the application, the attorney or State investigator is only required to identify himself and the law enforcement agency conducting the investigation and certify to the reviewing judicial official that the information likely to be obtained from the pen register or trap and trace device is relevant to an ongoing criminal investigation of that particular agency. The applicant does not have to set forth facts meeting any evidentiary standard. The applicant is only required to affirm the relevancy of the anticipated information to the criminal investigation.

Likewise, the reviewing judicial official makes no independent review of the relevancy of the information anticipated to be gained from the pen register or trap and trace device, but only ascertains that the submitted application is complete. Therefore, the applicant is not required to supplement the application with any factual affidavit. Upon receipt of the appropriate application, the court is to approve an order

"Law enforcement . . . has the responsibility to have both a working knowledge of the technical aspects of [communication facilities] and the legal requirements necessary to access the communications on the facilities and related records and information."

authorizing the identified law enforcement agency to use the requested pen register or trap and trace device.

The order, which should be prepared by the applicant and presented to the judicial official with the application, must include certain information: 1) The identities, if known, of the subscriber to the telephone to which the pen register or trap and trace device is to be attached and the person who is the subject of the criminal investigation; 2) the number, and if known, location of the phone to which the pen register or trap and trace is to be attached; and 3) the type of criminal activity being investigated.

The order will direct the appropriate telephone company to furnish the technical assistance necessary to accomplish the pen register or trap and trace. It will also direct the phone company not to disclose the existence of the pen register or trap and trace device to any person, to include the subscriber to the phone to which either type device is attached. The ECPA also requires the order be sealed from public access, so the subscriber of the targeted phone or the criminal under investigation cannot determine the existence of the device by perusing court records. The order is effective for 60 days, although the law enforcement agency may seek 60-day extensions of the order by repeating the same authorization procedure.[50]

The ECPA additionally requires the agency which uses the device to compensate the telephone company which has been directed to provide the necessary technical assistance for the reasonable value of that assistance. This includes costs reasonably incurred by the phone company for maintaining lines necessary for a pen register or trapping incoming phone calls.

Finally, Congress recognized that law enforcement officers principally use the trap and trace device in fast-moving criminal investigations, such as those involving kidnappings and extortions. In these types of investigations, the investigating officers seldom have sufficient time to obtain appropriate judicial approval for the use of a trap and trace device. Therefore, law enforcement officers may use trap and trace devices, as well as pen registers, and seek the necessary assistance from the appropriate telephone company after obtaining the consent of the user of the telephone to which the device is to be attached without obtaining judicial approval.[51]

Stored Communications and Transactional Records

As previously noted, the ECPA alters the law in three distinct aspects of the communications area. It not only requires the police officer: 1) To obtain a wiretap-type order to intercept electronic communications during the course of their transmission; and 2) to obtain prior judicial approval to use pen registers or trap and trace devices in the absence of consent; but 3) it also requires the officer to follow specific procedures when obtaining certain information from institutions which provide communication services to the public, such as telephone and computerized message companies.

The officer must follow this procedure to obtain both communications which have been stored by these service providers and transactional records of communication services which include billing information and nonpublic, or unlisted, subscriber information. That portion of the ECPA which sets forth this procedure is of immediate concern to all law enforcement officers, as it has applied to Federal, State, and local investigative activity since January 20, 1987. For this reason, all investigators should thoroughly acquaint themselves with this portion of the ECPA. The two types of records addressed by this portion of the ECPA are each discussed in turn below.

Billing Records and Nonpublic Listing Information

Billing records for telephone and similar communications services are frequently valuable sources of investigative information. These would include records maintained by a telephone company of toll, or long distance, calls made from a phone being used by the subject of a criminal investigation. These toll records not only indicate the numbers dialed in long distance calls but also the dates and times those calls were made. This information is frequently invaluable in ascertaining members of a wide-ranging criminal conspiracy and is often of evidentiary value. For example, long distance calls made from the phone of a narcotics distributor are frequently of assistance in identifying the distributor's sources and places of supply, customers, and money launderers.

Additionally, the criminal investigator will commonly find it necessary to determine from the telephone company the subscriber to, and location of, a certain phone number or the number and location of the phone of a certain subscriber. For example, the investigator may ascertain a certain phone number

is relevant in an investigation, as it was recorded on a pen register attached to the phone of the subject of an investigation. In such circumstances, it would be significant to determine the location of and subscriber to that particular number. If this subscriber information is not readily accessible to the public because it is unlisted, the law enforcement officer must obtain it from the appropriate telephone company. The ECPA defines the procedures the police officer must follow to obtain these types of nonpublic information pertinent to the customer of a communication service, in the absence of the consent of that customer.[52]

These procedures permit the law enforcement officer to obtain this information from the communications service provider, most often a public telephone company, in several ways. In the absence of the subscriber's or customer's consent, the officer must present the appropriate telephone company with one of the following: 1) A fourth amendment search warrant predicated upon a determination of probable cause by a neutral and detached magistrate, 2) a subpoena, or 3) a court order directing the company to provide the requested information.

The subpoena may be a Federal or State grand jury subpoena or an administrative subpoena, if Federal or State law allows the use of an administrative subpoena under those circumstances. An administrative subpoena is generally one which has been issued by the head of a law enforcement agency for specific investigative purposes. For example, Congress has given the Attorney General the power to issue administrative subpoenas in investigations of Federal narcotics violations pursuant to the Controlled Substances Act.[53] The Attorney General has, in turn, delegated this administrative subpoena authority to certain officials of the Drug Enforcement Administration and the Federal Bureau of Investigation. Agents of these Federal law enforcement agencies can thereby use properly obtained administrative subpoenas to acquire toll records and unlisted subscriber information from telephone companies in narcotics investigations.

If a law enforcement officer resorts to obtaining a court order to access toll records or nonpublic subscriber-related information, he must, in the application for such an order, make a factual showing that the requested records or information are relevant to an actual, or legitimate, criminal investigation. This relevancy standard is obviously much less than the probable cause standard required for a fourth amendment search warrant, but nonetheless requires some affirmative, albeit minimal, recitation of facts in the application.

The law enforcement agency which acquires this type of information does not have to provide any type of notice to the subscriber or customer to which the information pertains, whether the information is obtained by search warrant, subpoena, or court order. The agency or department normally also does not have to reimburse the company which provides the requested information for any costs incurred in processing the information, such as copying and labor costs, unless a court determines the amount of information to be unusually voluminous or the request to be unduly burdensome.[54] In order to facilitate the acquisition of this transactional information from the involved telephone company, however, the agency should attempt to arrive at a figure for reimbursement which is mutually agreeable to the phone company when the request is in fact unusually burdensome.

Stored Communications

As previously discussed in part one of this article, police officers must now obtain appropriate judicial approval in the form of a wiretap-type order to intercept either a wire or electronic communication *during the course of its transmission.* Numerous communications service companies, however, provide more services to their customers than just facilities for the transmission of telephone calls and electronic communications. One such service allows the customer to electronically send the communication to the service provider, which will store the communication for later transmission to the intended recipient.

For example, numerous providers of electronic communications services allow their customers to send an electronic communication through their computer terminals and modems to an electronic mailbox maintained by the service provider. The service company will store the computerized message and transmit it only when the intended recipient, or addressee, accesses the mailbox through his own computer, by relaying the proper access code to the service provider. Similarly, a phone company may store a voice communication in computerized, digitized form for retrieval by the intended receiver. Those companies which provide this mailbox service also routinely copy

". . . police officers must now obtain appropriate judicial approval in the form of a wiretap-type order to intercept either a wire or electronic communication during the course of its transmission."

these computerized messages and electronically store them for a short period of time in case of electronic difficulties or failures in the mailbox system. If a failure occurred, they would still be in a position to provide the message to the addressee.

The ECPA provides certain procedures available to the law enforcement officer to acquire contents of communications when they are stored by the electronics communication service company for purposes of later transmission to an intended recipient, in the absence of consent of a party to the communication.[55] In this regard, if the customer to this service electronically places the communication, or message, on what is known as an electronic bulletin board which is electronically accessible by the public through their computer terminals, the customer impliedly consents to the message's acquisition by all, including law enforcement. In the absence of consent, whether implied or actual, however, the police officer must comply with the ECPA's procedures when acquiring these types of stored electronic messages.

Congress has determined that when communications intended for eventual transmission to another have been stored in an electronic mailbox, or copied and stored by the service provider for fail-safe considerations, for a period of 180 days or less, they are akin to the contents of traditional mail and therefore deserve similar privacy protection. The officer, in the absence of consent of one of the parties to the message, can only access this type of stored communication in the same way he would access the contents of mail. He must present a search warrant predicated upon probable cause and obtained from a judicial official to the communication service provider. He does not, however, have to notify the affected customer that he is about to or has obtained the stored communication.

If, however, the communication service provider has electronically stored the message for a period of more than 180 days, the officer has several alternative means of acquiring it. He may use a search warrant, in which case he does not have to notify the affected customer or subscriber. He may also present to the electronic communication company a subpoena, which can be either a grand jury or administrative subpoena, or a court order directing the company to provide the requested messages. To obtain this court order, the officer must set forth, in his application, sufficient facts to show or convince the reviewing court that the messages which are sought are relevant to the criminal investigation. Again, this relevancy standard is less than a probable cause standard and should be satisfied by a minimal recitation of facts in the application.

If, however, the law enforcement agency attempts to obtain this type of stored communication by the use of a subpoena or court order, it must first notify the affected customer that it is requesting the messages from the customer's electronic communication, or computerized message, company. This is required so that the affected customer has the opportunity to contest the request by attempting to quash the subpoena or vacate the court order in the appropriate judicial forum. If the customer does not contest the acquisition, the computerized message company must release the requested information.

Under the appropriate circumstances, however, the agency or department may delay this notification requirement for a period of 90 days, and in the interim, receive the requested messages.[56] The agency may delay notifying the customer if the notification might adversely affect the criminal investigation. For example, the agency may delay notification if it might endanger the physical safety of an individual or cause an individual to flee from prosecution, destroy or tamper with evidence, or intimidate potential witnesses. The agency may thereafter extend the notification requirement every 90 days if similar circumstances continue to exist.

The means by which the department or agency accomplishes this delay in notifying the affected customer depends on whether the department seeks the electronically stored messages by subpoena or court order. If the investigative agency seeks the messages by subpoena, the head of the agency's regional office, or his first assistant, or the chief prosecuting attorney, or his first assistant, is only required to execute a written certification, or affirmation, that notification might have an adverse result. For example, the Special Agent in Charge or Assistant Special Agent in Charge of an office of the Federal Bureau of Investigation or the chief or assistant chief of a police department may certify this delay. The requesting agency may attach this certification to the subpoena itself. If, however, the department or agency seeks to obtain these messages by

court order, the court to which the application is made must make the determination that notification might lead to an adverse result. The requesting department would therefore have to make some assertions in its application for the order justifying this conclusion. Of course, once the period of delay, to include extensions, expires, the agency must present written notification of its acquisition of the stored electronic communications to the customer.

If the agency delays the notification, it may also obtain a court order commanding the electronic communication service provider to not notify any person, to include the affected customer, of the request for the electronically stored messages. The officer may obtain this order if the issuing court determines that the notification would again adversely affect the criminal investigation.[57]

Finally, with regard to stored communications, the ECPA defines the procedure law enforcement must observe to acquire records that have been electronically transmitted to a service providing company for purposes of storage or computer programming only.[58] For example, some electronic communications service companies offer a service to the public whereby their customers can transmit information through their own computer terminals and modems to the company. The company, in turn, maintains this electronically transmitted information in its computer bank for storage purposes only. It does not store the information for later transmission to another party, but only stores it for the sending customer without ever accessing it. It may, in some circumstances, electronically apply computer programs to the information, but otherwise simply leaves it in its computerized storage banks for later electronic retrieval by the sender.

In this manner, an individual involved in criminal activity might electronically transmit records of the criminal activity, such as narcotics distribution records, or records of fraudulent acquisitions to the service provider. The criminal is then in an extremely advantageous position. He can immediately access the recorded information through his computer terminal without physically possessing the records, which are electronically stored in the computer banks of the service company. If law enforcement officers were to search the criminal's residence or business, they would not likely, in such a situation, find any evidence of the criminal records. In such circumstances, the officers must obtain the incriminating records from the electronic communication storage company.

If the police officer obtains these types of records from the company which provides the electronic storage, he must follow the proscribed procedure of the ECPA. This procedure is exactly the same procedure law enforcement must follow when accessing electronic communications which have been stored for more than 180 days for the purpose of later transmission to another party, as previously discussed.

The officer may obtain these electronically transmitted records, which are being stored exclusively for storage purposes, by means of a search warrant. If the officer accesses this information by warrant, he does not have to provide the affected customer any prior notice of the acquisition. The officer may also obtain these records by use of a subpoena, grand jury or administrative, or a court order issued on a determination of relevancy, directing the computerized record storage company to provide the requested information.

If the officer relies upon a subpoena or court order, however, he must provide the affected customer prior notice of the acquisition, in order that the customer has the opportunity to contest the acquisition in a court of law. The officer can again delay this notice requirement for a period of 90 days, if it might adversely affect the criminal investigation, and during the delay, obtain the records. The appropriate law enforcement or prosecuting official must certify cause for the delay if the officer uses a subpoena to obtain this type of information. If, however, he obtains a court order, the authorizing judicial official must determine there is appropriate cause for delay.

If the law enforcement officer must provide the affected customer prior notice of the acquisition of the electronically stored information, he runs the risk that the customer, upon notification, might gain immediate access to the records through his computer terminal and either retrieve or erase them from the service company's electronic storage banks, before the company is able to copy them for the requesting officer. For this reason, the officer may, when requesting the records, also request the service provider to construct a backup copy of the records if, in his discretion, he believes that notification to the customer may result in tampering with evidence.[59]

In such circumstances, the service provider, without notifying the affected

"Under the provisions of the ECPA, an attorney of the government . . . or a State law enforcement officer must make written application, under oath, to a court of general criminal jurisdiction for proper authorization to use either a pen register or a trap and trace device."

customer, must produce this backup copy within 2 working days of the request and then advise the requesting officer that the reproduction has been completed. Once advised, the officer has 3 days to notify the customer unless, of course, the notification requirement has been properly delayed. If notified, the customer, in order to contest the acquisition, must seek the appropriate judicial remedy within 14 days. The records are therefore preserved if the customer attempts to electronically destroy them after notification. The service provider is also in a position to provide them to the requesting agency, whether the customer contests their acquisition or not.

CONCLUSION

Today's criminals are using sophisticated communications facilities in committing their illegal acts. Law enforcement therefore has the responsibility to have both a working knowledge of the technical aspects of these facilities and the legal requirements necessary to access the communications on the facilities and related records and information.

The ECPA provides common procedures for Federal, State, and local law enforcement officers to follow in discharging these duties. First, it requires a Federal officer to now obtain a wiretap-type order when nonconsensually intercepting an electronic communication. State and local officers with electronic surveillance abilities must do the same by October 2, 1988, unless, of course, their respective State law requires it sooner. Second, it requires Federal officers to also follow specific procedures in seeking authorization to use pen registers and trap and trace devices. Again, State and local officers must follow this procedure by October 1988, unless their State law is presently more restrictive or their State adopts the provisions of this portion of the ECPA before the October 1988, date. Finally, all officers, whether Federal, State, or local, must immediately observe the provisions of the ECPA when acquiring electronic communications stored by electronic communications service providers or information relating to the customers of communications services, such as toll records and unlisted subscriber information.

Because of these recent changes in the law and their resulting impact on law enforcement responsibilities, it is incumbent upon Federal, State, and local officers to acquaint themselves with these provisions of the ECPA. Moreover, law enforcement agencies should consider modifying any existing internal procedures or developing new ones as needed to achieve an ordered and effective compliance with ECPA requirements. They should also examine their liaison with communications service providers, such as telephone companies, to ensure that it is adequate to meet their fast-developing investigative needs pursuant to this statute. FBI

Footnotes

[42] *Supra* note 1.
[43] *Supra* note 39.
[44] *Supra* note 19.
[45] *Supra* note 20.
[46] 18 U.S.C. 3121-3126. Federal agents may also obtain authority to use pen registers and trap and trace devices pursuant to the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801-1811, in foreign counterintelligence investigations.
[47] *Supra* note 25.
[48] 18 U.S.C. 3122.
[49] 18 U.S.C. 3126(2).
[50] 18 U.S.C. 3123.
[51] 18 U.S.C. 3121(b).
[52] 18 U.S.C. 2703(c)(1)(B). Special Agents of the Federal Bureau of Investigation can also obtain this information upon written request of the Director, or his designee, in foreign counterintelligence investigations. 18 U.S.C. 2709.
[53] 21 U.S.C. 874.
[54] 18 U.S.C. 2706(c).
[55] 18 U.S.C. 2703(a).
[56] 18 U.S.C. 2705(a).
[57] 18 U.S.C. 2705(b).
[58] 18 U.S.C. 2703(b).
[59] 18 U.S.C. 2704.