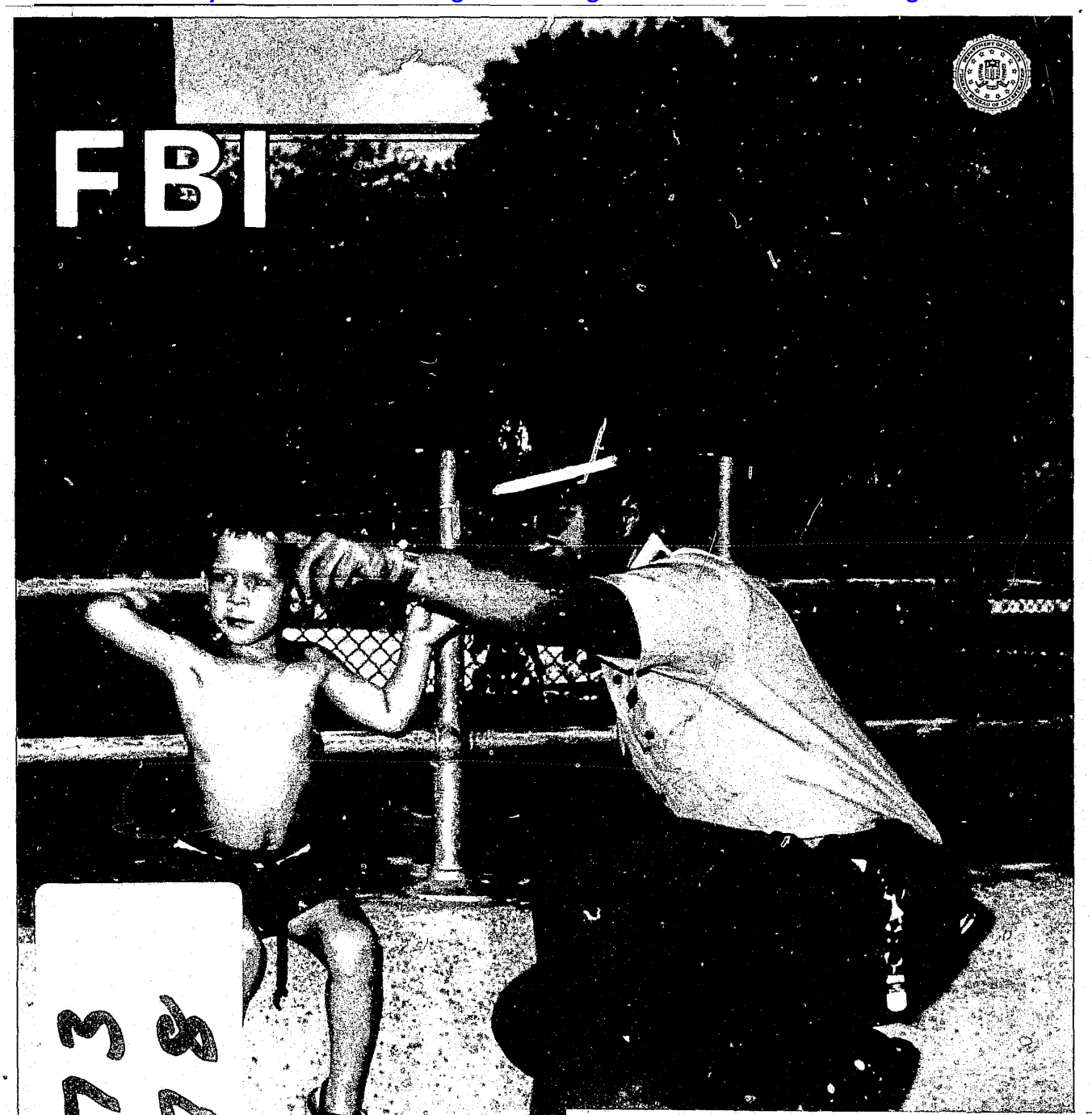

110273
110278

ce Cadet Corp

Contents

March 1988, Volume 57, Number 3

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—Mark A. Zettler

The Cover:

A police cadet gains field experience assisting a lost child (see article p. 1).

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

The Electronic Communications Privacy Act

Addressing Today's Technology

(Part II)

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 provoked Congress to pass the Electronic Communications Privacy Act of 1986[24] (the ECPA). Parts two and three of this article will address those three provisions of the ECPA which commonly impact Federal, State, and local investigative procedures. Part two will address that portion of the ECPA which now requires law enforcement officers to obtain extraordinary, or wiretap-type, orders when planning to nonconsensually intercept electronic communications, such as messages sent to digital display pagers or messages sent from one computer to another. Part three will discuss the two remaining provisions of the ECPA: (1) That portion which sets forth the procedure law enforcement officers must follow to use pen registers, which record the phone numbers dialed from a telephone, and trap and trace devices, which determine the origin of a phone call; and (2) the section of the ECPA which proscribes the procedure police officers must observe when obtaining stored electronic communications, such as computerized messages kept in an electronic mailbox, and transactional records of communications services, to include telephone toll records and nonpublic telephone subscriber information.

THE ECPA

When considering these three separate provisions of the ECPA, State and local law enforcement officers must first understand two significant points that affect their work in this area. First, the ECPA is not intended to preempt existing State law, whether of statutory or judicial origin.[25] For example, if the State standard or procedure for obtaining toll records or using pen registers is more restrictive than that provided for by the ECPA, police officers within that State must comply with the stricter State law.

Second, although all three sections of the ECPA have been applicable to Federal investigations since the ECPA's effective date, January 20, 1987, they affect State and local investigations at varying times. The third section of the ECPA to be discussed in this article, involving government access to stored communications, toll records, and unlisted subscriber information, had universal effect on

Special Agent Fiatal

January 20, 1987. State and local officers must therefore understand and comply with this portion of the act immediately.

Congress determined, however, that the first section of the ECPA, requiring the acquisition of a wiretap-type order to intercept electronic communications during their transmission, and the second section to be discussed, setting forth the procedure law enforcement must follow to use pen registers and trap and trace devices, were significant changes in traditional law. Therefore, States will have 2 years from the date of enactment of the act to bring their own law into conformity with those two provisions of the ECPA.[26] As Congress passed the act on October 2, 1986, State and local officers have to comply with these two sections of the ECPA by October 2, 1988, unless, of course, their respective States adopt procedures in these areas at least as restrictive as the Federal mandates before October 1988.

Interception of Electronic Communications

As discussed in part one of this article, prior to the enactment of the ECPA, Title III of the Omnibus Crime Control and Safe Streets Act [27] (title III) and its analogous State statutes required law enforcement officers to obtain extraordinary judicial orders when they planned to aurally intercept wire communications (wiretaps) or oral communications where there exists a reasonable expectation of privacy (bugs), in the absence of the consent of a party to the communication. An aural interception was the interception of a communication involving the transmission of the human voice. Title III therefore provided no protection to communications that did not involve the spoken word, such as telegraph or facsimile-type communications, which involve the electronic transmission of a written message, photograph, drawing, or document.

The first portion of the ECPA significantly expanded the traditional wiretapping and bugging law by also affording the same protections previously supplied to wire and oral communications to electronic communications. The ECPA provides that in order to intercept an electronic communication during the course of its transmission, without the consent of one of the parties to that communication, the police officer must obtain an extraordinary order, just as if he were intercepting a wire communication or an oral communication involving a reasonable expectation of privacy.[28] Although this portion of the ECPA immediately affected Federal wiretapping procedure, State and local officers are not required to conform with this change in the law until October 2, 1988.

In effecting the expansion of the traditional wiretapping and bugging law, Congress provided a very broad definition of what is an electronic communication. It basically includes any type of communication transmitted by some electronic means, unless it involves the transmission, at least in part, of a human voice, which would instead be a wire communication. This broad definition of an electronic communication encompasses those written messages, documents, and photographs transmitted by telegraph and facsimile-type communications services. It also includes those communications electronically transmitted from one computer

". . . States will have 2 years from the date of enactment of the act to bring their own law into conformity with . . . two provisions of the ECPA."

terminal to another and those numerically coded messages transmitted to digital display paging devices. If a law enforcement officer intends to intercept any of these types of communications during the course of their transmission and does not have the consent of one of the parties to the communication, he must first obtain an interception, or wiretap-type, order. He must of course fulfill the same procedural requirements in the application for such an order as if it were an application for the interception of wire or oral communications.[29] These include the traditional probable cause and particularity requirements, as well as an explanation of exhaustion of traditional investigative techniques and a record of prior interceptions and interception efforts.

When constructing such an all-inclusive definition of electronic communications, Congress realized that there were several types of communications that, although technically falling within the definition of an "electronic" or "wire communication," did not deserve those protections afforded by title III. Congress therefore created several exceptions to what might otherwise be deemed an "electronic" or "wire communication," and each is noted in turn.

Communications Not Protected by the ECPA

The ECPA expressly denotes six types of communications for which a law enforcement officer is not required to obtain a wiretap-type order to intercept. Some fourth amendment consideration may, however, be applicable in limited circumstances, as the interception may involve the government's intrusion into a reasonable expectation of privacy. If so, the law enforcement officer must obtain a search warrant in the absence of consent or emergency. While analyzing the ECPA's six exceptions to electronic and wire communications, this article will also address any possible fourth amendment considerations applicable to those exceptions.

Publicly accessible radio communications

Law enforcement officers and others can receive, or intercept, radio transmissions which are "readily accessible to the general public"[30] without obtaining a wiretap order. This would include interception of AM-FM radio broadcasts and those ham radio broadcasts, CB broadcasts, walkie-talkie broadcasts, and marine or aeronautical, or ship to shore, broadcasts, which are not scrambled or encrypted in such a manner as to thwart their public accessibility.

Tracking devices

Police officers can also monitor tracking devices, sometimes referred to as beacons, or beepers, without obtaining a wiretap order.[31] Tracking devices emit periodic radio signals which enable the receiver to ascertain the movement of the device. Law enforcement agencies commonly attach these devices to a motor vehicle, airplane, or boat or place them in a package containing narcotics or chemicals or equipment used to manufacture narcotics, so that they may monitor the movements of the vehicle or package.

Although the police officer is not required to obtain a wiretap order to monitor the transmissions of these types of devices, he may, under certain circumstances, infringe upon an individual's reasonable expectation of privacy by monitoring such a device. In *United States* v. *Knotts*,[32] the Supreme Court determined that when a law enforcement officer monitors the movements of a tracking device while it is upon the highway, or within public view, he does not infringe upon an individual's reasonable expectation of privacy, as the individual has no such expectation of privacy in his movements in publicly visible areas. The police officer therefore does not need a search warrant when confining his monitoring of the tracking device to such circumstances.

In the subsequent case of *United States* v. *Karo*,[33] however, the Supreme Court recognized that if a law enforcement officer continued to monitor the tracking device once it moved into an area where it was no longer within public view, such as inside a residential premises, and obtained information which he could not have obtained by lawful visual surveillance, he was intruding into a justifiable expectation of privacy. In this situation, the police officer needed a search warrant to continue to monitor the device, in the absence of an emergency, to comply with fourth amendment requirements.[34]

Radio portion of cordless telephones

As previously mentioned, handheld cordless telephones have become overwhelmingly popular with the public. When purchased, a warning on the packaging of such a device advises the buyer that other individuals can easily intercept the conversations made over the device. They may accomplish this by using a similar device, and in some

instances, a standard AM-FM radio receiver. Congress duly recognized that there was little, if any, privacy interest in that portion of a communication which travels over radio waves between the cordless phone and the base unit. The law enforcement officer, therefore, is not required to obtain judicial approval to intercept the radio portion of a communication made over a handheld cordless telephone.[35] Likewise, the officer does not have to obtain a search warrant to overhear the radio portion of a cordless phone, as such activity does not intrude into a reasonable expectation of privacy.

It should be pointed out in this context that unlike the radio portions of cordless phone communications, those communications made through cellular phones are wire communications. The law enforcement officer must therefore obtain a wiretap order to intercept this type of communication in the absence of consent of one of the parties to the cellular phone call. This even includes calls made from one cellular phone to another cellular phone.[36]

Although portions of the cellular phone call, like portions of the cordless phone call, travel over the airwaves, there are valid reasons for this distinction. Cellular phones have a far greater range -- sometimes hundreds of square miles, due to the number of radio receivers and transmitters arranged in adjacent geographical areas — than the range of cordless phones, commonly limited to a few hundred feet. Additionally, the type of equipment needed to intercept a cellular phone call is much more sophisticated and expensive than that needed to intercept the radio portion of a cordless phone, due to the range capabilities of the cellular phone and the varying radio frequencies used in such transmissions. Persons therefore possess a much higher expectation of privacy in calls made over a cellular phone than in those made over a cordless phone.

Tone-only paging devices

A police officer may intercept the transmission made to a tone-only paging device without obtaining a wiretap order.[37] As previously noted, there is no expectation of privacy in the beep made through such a device that merely notifies the possessor of this type of pager that someone is attempting to reach him. The officer therefore also need not acquire a search warrant to conduct such an interception as this activity does not involve an infringement upon any legitimate expectation of privacy.

The criminal who relies upon paging services to facilitate his illegal activities, however, seldom uses a tone-only pager. Instead, he will use a voice pager, or more frequently, a digital display paging device. Those involved in the illicit transfer of narcotics often contact their buyers and providers through digital display pagers. As discussed elsewhere, in contrast to the tone-only pager, those communications transmitted to a voice pager are wire communications as they involve the spoken word. Also, those communications sent to a digital display pager fall within the definition of electronic communications. Therefore, the law enforcement officer must obtain proper judicial authority by obtaining a wiretap-type order before intercepting messages sent to a voice or display paging device, in the absence of consent of a party to the communication.

Surreptitious video surveillance

If law enforcement officers desire to intercept a closed-circuit television broadcast during its transmission, for example, a video teleconference between two suspected criminals, they must first obtain an interception order. The intercepted television transmission would be an electronic communication, now entitled to the protections afforded by title III. If the officers merely survey a suspected criminal through the use of a video camera, however, they do not have to comply with wiretap procedure. They are not tapping, or intercepting, any type of electronic, wire, or oral communication.

If the officers use the video equipment to watch an area or activity where the person or persons observed have a reasonable expectation of privacy, they will, however, need to obtain a fourth amendment search warrant, unless they have the consent of one of the parties and that party is present while the officers conduct the surveillance. Two U.S. circuit courts of appeal, recognizing this type of video surveillance to be unusually intrusive, have recommended that the applications for video surveillance search warrants and the search warrants themselves satisfy certain procedural requirements also found in title III.[38] For example, these circuit courts stated that applications for video surveillance warrants should explain that less-intrusive investigative techniques, like the use of informants, undercover officers, or traditional search warrants, have been tried and failed or why they would be unlikely to succeed or be unnecessarily dangerous. Additionally, these courts require

". . . the ECPA is not intended to prempt existing State law . . . if the State standard or procedure . . . is more restrictive than that provided for by the ECPA, police officers within that State must comply with the stricter State law."

video surveillance warrants to be effective for no more than 30 days. The orders must also, like a wiretap order, particularly describe the people, place, and type of criminal activity to be observed and instruct the executing officers to minimize their interception of innocent, or noncriminal, activities. If the officers, in conjunction with nonconsensual video surveillance into an area where there exists a reasonable expectation of privacy, also intercept the oral communications of those viewed by a hidden microphone, they must, of course, obtain a "bug" order pursuant to title III or analogous State law to lawfully intercept the oral communication, in addition to the video surveillance warrant.

Pen registers and trap and trace devices

The ECPA specifically states that law enforcement officers are not required to obtain a wiretap-type order to use pen registers, which record the numbers dialed from a telephone, and trap and trace devices, which determine the point of origin of a telephone call.[39] As previously discussed, the Supreme Court also determined that there is no reasonable expectation of privacy in the numbers dialed from a telephone.[40] Therefore, police are also not required to obtain a search warrant to use a pen register or trap and trace device.[41]

Although police are not required to obtain a wiretap order or a search warrant to use either pen registers or trap and trace devices, phone companies, who provide necessary technical assistance in using these types of investigative techniques, commonly insist in nonemergency situations upon some type of court authorization before providing their assistance. Congress, in order to set forth a standardized procedure for obtaining 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, set forth specific procedures that police officers must follow to obtain authorization for their use.

They must either obtain a court order, to be issued upon the applicant's assurance or affirmation, that the information to be gained from the pen register or trap and trace device is relevant to a legitimate criminal investigation or consent from the user of the telephone to which the device is to be attached.

Part three of this article will discuss in detail this portion of the ECPA which proscribes procedures for using pen registers and trap and trace devices. It will also examine that portion governing the acquisition of stored communication, such as those in electronic mailbox systems, and information pertaining to the subscriber of a communication service, such as telephone toll records and nonpublic telephone listing information.

FBI

(Continued next month)

Footnotes

[24]*Supra* note 1.

[25]18 U.S.C. 2703 and 3122(a)(2).

[26]Senate Bill 2575, 99th Congress, 2d Session, Electronic Communications Privacy Act, Sections 111 and 362.

[27]*Supra* note 3.

[28]18 U.S.C. 2511(1).

[29]The ECPA does, however, somewhat relax the procedure a Federal law enforcement officer must follow to apply for a court order authorizing the interception of an electronic, rather than a wire or oral, communication. The application for such an order can be predicated upon the investigation of any Federal felony and can be authorized for transmittal to a Federal judge by any U.S. attorney. 18 U.S.C. 2516(3). Nonetheless, the Department of Justice, as a matter of policy, will continue to require departmental application approval for electronic communication interception orders for 3 years from the effective date of the act.

[30]18 U.S.C. 2510(16) and 2511(2)(g).

[31]18 U.S.C. 2510(12).

[32]460 U.S. 276 (1983).

[33]468 U.S. 705 (1984).

[34]For a more detailed discussion of the fourth amendment's application to the monitoring of tracking devices, see John C. Hall, "Electronic Tracking Devices: Following the Fourth Amendment," *FBI Law Enforcement Bulletin*, vol. 54. No. 3, (Part I) February 1985, pp. 26-31; No. 4, (Conclusion) March 1985, pp. 21-31. The ECPA does provide for the potential extraterritorial jurisdiction of a search warrant issued to monitor a tracking device. If obtained, the warrant can be effective even if the device moves out of the jurisdiction in which the warrant was issued, as long as the device was installed within the issuing jurisdiction. 18 U.S.C. 3117.

[35]18 U.S.C. 2510(1) and (12).

[36]18 U.S.C. 2510(1) defines a wire communication to include those voice communications that are transmitted through switching stations.

[37]18 U.S.C. 2510(12).

[38]See *United States* v. *Biasucci*, 786 F.2d 506 (2d Cir. 1986); *United States* v. *Torres*, 751 F.2d 875 (7th Cir. 1984).

[39]18 U.S.C. 2511 (2)(h).

[40]*Supra* note 19.

[41]The Supreme Courts of the States of Colorado and Pennsylvania have determined the use of a pen register to be a search under their respective State constitutions and therefore require that officers obtain a search warrant prior to their using such a device, in the absence of consent or emergency. *Commonwealth* v. *Beuford*, 475 A.2d 783 (Pa. Sup. Ct. 1984); *People* v. *Sporleder*, 666 P.2d 135 (Col. Sup. Ct. 1983).