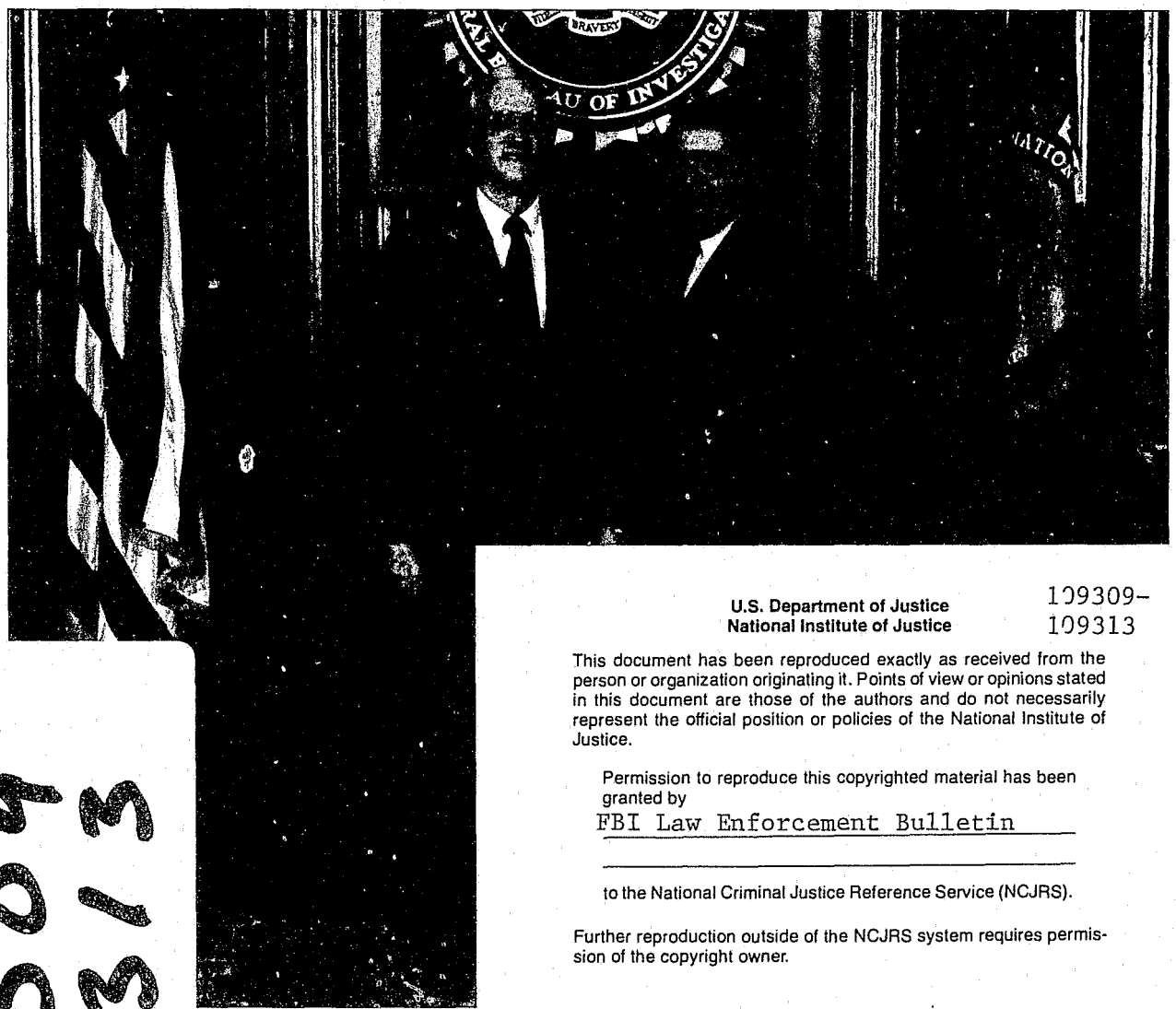

Contents

February 1988, Volume 57, Number 2

109309
109310
109311
109312
109313

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:

Director William S. Sessions meets Julien C. Gallet, the new President of the FBI National Academy Associates.

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 1)

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.

In our fast-moving society, criminals will always take advantage of all available communications facilities to conduct their illegal activity. Not only do they use telephones to participate in fraudulent business transactions or drug deals, but they also use more-sophisticated communication devices, including paging devices, which deliver a signal or message to their users; cellular telephones, which can be transported in cars and briefcases; and electronic communication systems, which transmit a message from one computer terminal to another.

It is, therefore, incumbent upon law enforcement officers to have both practical knowledge as to how these communication devices and services work and an understanding of how they can lawfully access, or intercept, communications made over these systems. Similarly, police officers need to know the legal requirements to obtain information related to the use of these communications facilities, such as telephone toll records and nonpublic information concerning the name and location of a subscriber to a communications service.

The Electronic Communications Privacy Act of 1986 (the ECPA)[1] significantly alters the procedure that Federal, State, and local law enforcement officers must follow to intercept communications during the course of their transmission and to acquire transactional information of those communications, such as telephone toll records. For these reasons, law enforcement officers must understand the impact of the ECPA on their investigative efforts in the communications area.

The ECPA consists of three distinct provisions. First, it amends the law of nonconsensual interception of wire communications (wiretaps) and oral communications by a concealed microphone or electronic device (bugs). Second, it sets forth specific procedures for obtaining authorization to use pen registers (telephone decoders), which record the numbers dialed from a telephone, and trap and trace devices, which ascertain the origin of a telephone call. Third, it proscribes the procedure law enforcement officers must follow to obtain certain stored communications and records relating to communications services, such as telephone toll records and unlisted telephone subscriber information.

Special Agent Fiatal

It is the purpose of this three-part article to acquaint the law enforcement officer with: 1) The reasons for passing this new Federal legislation; 2) significant provisions of the ECPA, which apply to Federal as well as State and local law enforcement activity; and finally 3) the effect of those provisions on Federal, State, and local investigative procedure.

The first part of this article will discuss those problem areas that led to the passage of the ECPA. Part two will specifically address that portion of the ECPA which changes the law of nonconsensual wiretapping. Part three will consider those portions which refer to law enforcement's use of pen registers and trap and trace devices and the acquisition of stored communications and information pertaining to the customers of communications services.

ELECTRONIC SURVEILLANCE PRIOR TO THE ECPA

Prior to the passage of the ECPA, a law enforcement officer who planned to conduct electronic surveillance, such as wiretapping or bugging, had to proceed under two legal constraints that remain in effect today. First, the fourth amendment prohibits "unreasonable searches and seizures."[2] Second, Title III of the Omnibus Crime Control and Safe Streets Act of 1968[3] (title III), or its State counterparts which either adopt the provisions of title III or set forth their own requirements, regulate the use of electronic surveillance.[4] To date, 31 States have enacted such counterparts,[5] which must be at least as restrictive as the provisions of title III.[6]

Fourth Amendment Considerations

The Supreme Court, in the landmark case of *Katz* v. *United States*,[7] which involved electronic surveillance in the form of a concealed microphone used to intercept a conversation, defined a search for purposes of the fourth amendment. In *Katz*, Agents of the Federal Bureau of Investigation, having reason to believe Katz was using a certain public telephone to transmit wagering information interstate, placed a surreptitious listening and recording device on top of and outside the phone booth without the benefit of prior court approval. The Agents thereafter intercepted Katz' end of his telephone calls made from that location and used them against Katz at his subsequent criminal prosecution.

Abandoning earlier decisions which equated a search with a physical trespass onto an individual's property, the Supreme Court determined that a search, for purposes of the fourth amendment, was any governmental intrusion into a person's legitimate, or reasonable, expectation of privacy, since that constitutional provision "protects people, not places."[8] The Court further determined that a search is reasonable by fourth amendment standards if it is conducted pursuant to search warrant or if it fits into one of the few specifically established exceptions to the general requirement of a warrant, such as a search incident to arrest, a motor vehicle exception search, or an emergency search. Finding the Agents' activity to constitute a search, the Court deemed it unreasonable as it was not executed pursuant to a search warrant and did not fall into one of the exceptions to this requirement as recognized by prior decisions of the Court.

"The Electronic Communications Privacy Act of 1986 . . . significantly alters the procedure that Federal, State, and local law enforcement officers must follow to intercept communications . . . and to acquire transactional Information . . . ."

The Supreme Court has also determined that when one of the parties to a conversation consents to have that conversation monitored, that activity does not constitute a search by fourth amendment standards.[9] For example, law enforcement officers may have the consent of one of the parties to a conversation to permit them to electronically survey, or intercept, that conversation. The nonconsenting party voluntarily exposes the information to the consenting party and assumes the risk that the consenting party may disclose the conversation to the police. The consenting party might accomplish this by either repeating or transmitting the information to the officers or recording it by the use of a surreptitious device. Therefore, the police officer need not obtain a search warrant in order to comply with the fourth amendment when one of the parties to the intercepted communication consents to its interception.

Title III or Its State Counterparts Requirements

Title III and its analogous State statutes provide that a law enforcement officer must obtain prior court approval before he aurally intercepts a wire communication or an oral communication involving a reasonable expectation of privacy, absent the consent of one of the parties to the communication.[10] The officer complies with title III or its State counterparts by following prescribed procedures to obtain the appropriate wiretap or bug order that permits the interception.

These procedures require the application for the order to include certain data. First, it must contain sufficient information to establish probable cause that an individual is committing or is about to commit certain specific criminal offenses and that the individual is also using the telephone to be tapped or the area to be bugged to transmit communications about that offense. Second, it must particularly describe the offense being committed, the individual (if known) whose communications are to be intercepted, the type of communication to be intercepted, and the phone to be tapped or the area to be bugged. Third, it must explain that other more traditional and less-intrusive investigative techniques, such as the use of informants, undercover officers, search warrants, physical surveillance, or grants of testimonial immunity, have been tried and failed or why they would be unlikely to succeed or be too dangerous. Finally, it must list all previous applications for interception of communications of the same individual or for the same phone to be tapped or area to be bugged.[11] Once obtained, the order is effective for a time period not to exceed 30 days.[12]

New Technology and Varying Judicial Interpretations Necessitating Additional Legislation

Since 1968, however, when title III became effective, the types of communications facilities and their technological sophistication have changed dramatically. Today, even the simple telephone call is seldom transmitted exclusively over wire. Frequently, a telephone call, at some point during its transmission, travels through microwave radio transmissions and sometimes is even transmitted via satellite. Fortunately, the provisions of title III covered such situations, as they prohibited, absent prior judicial approval, the nonconsensual aural interception of wire communications transmitted in whole *or part* through the wires.[13] These technological advances, however, created many other issues involving law enforcement's use of electronic surveillance and acquisition of information relating to communications which were unaddressed by title III. Since they were not specifically addressed by statutes, they received varying judicial treatment in State and Federal courts, and this created some confusion for law enforcement investigative procedures. Each of these technologically advanced communication devices is discussed in turn below.

Cellular and Cordless Telephones

The cellular telephone is a prime example of a technologically advanced communication facility which has rapidly gained increased public popularity. An individual can easily transport a cellular telephone device in a motor vehicle or briefcase. Any call made from such a device travels, by radio wave, to the nearest receiver maintained by the cellular telephone company. The call is thereafter transmitted, again by radio waves, to the central receiver of the cellular telephone company, where it then enters the wires of the public telephone company for further transmission to a land-line, or traditional, telephone. Although title III did not specifically address calls from a cellular to a land-line phone or from a land-line to a cellular telephone, these calls are at least transmitted in part by wire and therefore deserved title III protection.[14]

The same rationale, when applied to the calls to or from a handheld cordless telephone, suggests that they deserve title III protection, but closer examination reveals that protection to be unwarranted. A handheld cordless

"The Supreme Court has . . . determined that the user of a telephone has no reasonable expectation of privacy in the numbers dialed from that phone."

phone transmits and receives communications sent by radio waves to and from a base unit maintained in the user's residence, where the call thereafter travels through the wires of the telephone company. A handheld cordless phone, unlike the cellular phone, has limited range, as the radio transmissions to and from such a device are ineffective beyond a relatively short distance. Additionally, persons who are not intended parties to the conversation can easily intercept these transmissions by using a similar device or an AM-FM radio receiver, which happens to be located nearby. Warnings on the boxes of newly purchased handheld cordless phones even advise the purchasers that other persons can easily overhear their conversations made over that device.

This ease of interception dramatically contrasts with the need to use a comparatively sophisticated interception device to overhear calls to and from a cellular telephone. For these reasons, although a portion of any such communication to or from a handheld cordless phone travels in part over wire, at least two State courts have rejected the necessity of obtaining a wiretap order to intercept communications to and from this device,[15] as there is little if any reasonable expectation of privacy in such transmissions.

Paging Devices

The paging device is another example of a communication facility whose use has not only become increasingly popular but also in certain format has outdistanced traditional title III concepts. The paging device emits a message which the provider of the paging service has transmitted over radio waves to the pager. These paging devices are of three types: 1) Tone-only pager, 2) voice pager, and 3) digital display pager.

A person who wishes to alert the possessor of a tone-only paging device simply calls the paging service company and leaves a message. The paging service company in turn transmits a simple radio signal to the tone-only paging device, causing the device to beep. This beep alerts the possessor of this type of pager to contact either the paging service company for the message or a predetermined place or individual.

Traditional title III provisions required the law enforcement officer to obtain a wiretap or bug order when he *aurally* intercepted a wire or oral communication.[16] An aural interception involves the interception of a communication understood and comprehended by the human ear or a communication involving the human voice. Congress did not intend the unamended title III to address nonvoice communications. Therefore, if a police officer intercepted the tone transmitted to a tone-only pager, he did not aurally intercept a spoken communication, and therefore, was not required to comply with the provisions of title III or its State counterparts. Additionally, inasmuch as an individual has no reasonable expectation of privacy in the transmission of a mere tone over radio waves, the law enforcement officer did not have to obtain a search warrant to intercept transmissions made to a tone-only pager because this activity is not a search by fourth amendment standards.

The voice pager, however, does involve the transmission of a spoken communication. The person who wishes to contact the possessor of this type of paging device calls the paging service and repeats a spoken communication, which is transmitted by the paging company over the air waves to the pager, allowing the possessor of the device to hear the spoken message. The nonconsensual interception of such a message involves the acquisition of a spoken communication, made at least in part through wire, necessitating title III protection. Nonetheless, one State supreme court which addressed law enforcement's interception of communications to a voice paging device believed that both the framers of title III and the State wiretap legislation did not intend them to cover the interception of communications to voice pagers.[17]

Finally, the digital display pager operates in a manner similar to the voice pager, except that the caller, after dialing the number of the paging service company, continues to dial a coded message, which the paging company transmits, by radio waves, to the intended pager. The paging device then displays the message. A police officer who intercepted a message to a digital pager did not intercept a communication protected by traditional title III standards, as the officer did not aurally intercept a communication. He acquired a numeric printout, rather than a spoken message. It would appear, however, that the individuals who either send or receive this coded signal possess a reasonable expectation of privacy in the message and deserve some type of legal protection.

Electronic Communications and Computer Messages

The interception of communications made over other types of techni-

cally advanced communications facilities, which do not involve the transmission of the human voice, sometimes known as electronic mail systems, was also outside the protection of traditional wiretapping statutes. There are numerous communications facilities that transmit written or typed messages and facsimiles of documents, drawings, or photographs, rather than spoken messages. The parties to these types of communications would nonetheless have an expectation of privacy in the electronic communication, just as they would in a telephone conversation.

Perhaps one of the most significant advances in communications technology, however, is the computerized communication system. In this type of system, an individual uses a computer terminal and modem to transmit written, digitized messages over wire and radio waves to another computer terminal. Under traditional wiretap law, however, the police officer was not required to obtain a judicial wiretap order to intercept communications made over these types of facilities, as the interception did not involve the acquisition of spoken messages. Nonetheless, the parties to such communications would appear to have the same expectation of privacy in these messages as they would in a common telephone call.

There were yet other matters concerning law enforcement's acquisition of information from public communication service providers that were unaddressed by any Federal legislation. Numerous communication service companies provide to the public what is sometimes called an electronic mailbox service. The customer of such a service may, if he wishes, transmit his computerized message to an electronic mailbox, best described as an electronic mail drop, maintained by the service provider. Later, the intended receiver may access the mailbox through his computer and thereby retrieve the message.

Additionally, the companies who provide this service routinely electronically copy and store these messages for a period of time as a safeguard against the failure of the electronic mailbox system. The provider of the service would then be in a position to retrieve the stored communication for its customers if the computerized electronic mailbox crashed or failed. Again, neither title III, passed in 1968, nor any other Federal or State legislation governed law enforcement's access to these messages, which could contain valuable investigative information, while they were in electronic mailboxes or when they were copied and stored by the service provider, for purposes of later transmission to the intended recipient.

Computerized message companies also frequently provide another service to their customers whereby the customer may transmit records and information electronically, by the use of computers and modems, to the service provider, exclusively for storage purposes. For example, an individual could maintain records of criminal activity in the storage banks of this type of computer service company, rather than at his own business or residence, and still be able to retrieve them instantaneously through his computer terminal. Again, no statute addressed law enforcement's acquisition of these records while in the possession of the service provider exclusively for storage purposes.

Pen Registers and Trap and Trace Devices

Title III was completely silent regarding the government's use of pen registers, or dialed number recorders, and trap and trace devices. These devices allow police to acquire the telephone numbers dialed from a telephone or the number of a telephone from which a call originates. As the use of either device did not involve the interception of spoken messages, it did not bring into play traditional title III protections and procedure.[18]

The Supreme Court has also determined that the user of a telephone has no reasonable expectation of privacy in the numbers dialed from that phone.[19] The user could reasonably expect that others, in particular the telephone company, would commonly use such devices for a variety of reasons, to include confirming proper billing information. Therefore, a law enforcement agency or department could use a pen register, through the cooperation of the appropriate phone company, without first procuring a search warrant. Similarly, when one dials a number on the telephone, he voluntarily provides the telephone company, a third party, the number of the phone he is dialing and assumes the risk that the telephone company may provide the number and location of the phone from which the call originated to the police.[20] Nonetheless, telephone companies frequently requested that law enforcement officers obtain some type of court order when seeking the telephone company's cooperation in using these devices. No law, however, proscribed the procedure to be followed in obtaining such an order.

". . . the ECPA amends title III to require a law enforcement officer to obtain an extraordinary wiretap-type order to nonconsensually intercept electronic communications."

Accessing Transactional Records (Telephone Toll Records)

Finally, law enforcement officers often find it useful in their investigations to obtain records from telephone companies of their customers' toll, or long distance, calls. These records are frequently used to determine other members of an organized criminal conspiracy, such as a narcotics distribution network. Similarly, the police, on a frequent basis, need to obtain from telephone companies nonpublic listing information, such as the name and address of the subscriber to a particular telephone number or the phone numbers of a particular subscriber. Again, no statutory standards governed law enforcement's acquisition of transactional records of communications services or information pertaining to the subscriber of a communications facility, when that information was not readily available to the public.

Faced with unaddressed or inconsistently addressed legal issues arising from these communications devices and records, Congress attempted to resolve these problems by passing the ECPA. Accordingly, the ECPA changes the law in three distinct areas which are of common significance to Federal, State, and local investigators. First, the ECPA amends title III to require a law enforcement officer to obtain an extraordinary wiretap-type order to nonconsensually intercept electronic communications.[21] This includes the interception of messages sent to digital display pagers and messages sent from one computer to another. It also, however, specifically excepts the interception of various communications from this requirement; these exceptions include the interception of messages sent to a tone-only pager and the radio portion of cordless telephone conversations.

Secondly, the ECPA requires the law enforcement officer to follow specific statutory procedures before using pen registers, as well as trap and trace devices.[22] He must obtain either a court order, by certifying to the issuing court that the device is necessary to his investigation, or consent from the user of the phone to which the pen register or trap and trace device is attached.

Finally, the ECPA addresses issues involving public communications service providers. It defines the procedure the police officer must follow when acquiring communications stored by a communications service provider for later transmission, such as computerized messages maintained in an electronic mailbox, or when acquiring computerized information electronically transmitted to a service provider exclusively for purposes of storage.[23] This particular section, however, also defines the requirements a law enforcement officer must meet to acquire certain information from a public communications service provider about their subscribers or customers. This type of information includes telephone toll records and nonpublic, or unlisted, subscriber information or that information disclosing the identity and address of the subscriber to a particular telephone number which is not available to the public. As law enforcement officers routinely access telephone toll records and unlisted information from telephone companies during the course of their investigations, they need to possess a thorough understanding of this particular section of the act.

Parts two and three of this article will examine these three distinct provisions of the ECPA.

(Continued next month)

Footnotes

[1]Public Law 99-508.

[2]U.S. Const. amend. IV provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3]Public Law 90-351.

[4]18 U.S.C. 2516(2) requires States to enact their own specific enabling statute if they desire to implement the authority granted State law enforcement officers by title III to seek and obtain electronic surveillance orders from State judges.

[5]Report of the Director of the Administrative Office of the U.S. Courts on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report) at 2 (1986).

[6]*See, United States* V. *Geller,* 560 F. Supp. 1309 (E.D. Pa. 1983); *State* v. *Thompson,* 464 A.2d 799 (Conn. Sup. Ct. 1983); *Commonwealth* v. *Vitello,* 327 N.E.2d 819 (Mass. Sup. Ct. 1975); *State* v. *Siegel,* 292 A.2d 86 (Md. Ct. App. 1972).

[7]389 U.S. 347 (1967).

[8]*Id.* at 351.

[9]*United States* v. *White,* 401 U.S. 745 (1971).

[10]18 U.S.C. 2511. A few States, enacting legislation more restrictive than title III, either limit or prohibit consensual monitoring in the absence of prior judicial approval.

[11]18 U.S.C. 2518(1).

[12]18 U.S.C. 2518(5).

[13]18 U.S.C. 2510(1).

[14]*See United States* v. *Hall,* 488 F.2d 193 (9th Cir. 1973).

[15]*State* v. *DeLaurier,* 488 A.2d 688 (R.I. Sup. Ct. 1985); *State* v. *Howard,* 679 P.2d 197 (Kan. Sup. Ct. 1984). It is noteworthy, however, that both these cases involved use of the intercepted handheld cordless phone communications as evidence against the party who used the handheld cordless phone. They did not address the situation where the intercepted conversations are used against the individual who used the traditional telephone in the land-line end of the conversation.

[16]Senate Report No. 1097, 90th Congress, 2d Session, at 90.

[17]*Dorsey* v. *State,* 402 S.2d 1178 (Fla. Sup. Ct. 1981).

[18]*See, United States* v. *New York Telephone Company,* 434 U.S. 159 (1977).

[19]*Smith* v. *Maryland,* 442 U.S. 735 (1979).

[20]*See, e.g., United States* v. *Miller,* 425 U.S. 435 (1976); *United States* v. *White, supra* note 10.

[21]18 U.S.C. 2510-2520.

[22]18 U.S.C. 3121-3126.

[23]18 U.S.C. 2701-2710.