AN OVERVIEW OF ELECTRONIC SURVEILLANCE IN THE UNITED STATES; LAW, POLICY, AND PROCEDURE

*Julie P. Wuslich**

I. INTRODUCTION

In the United States, there are two primary levels of government—the federal system and the state system.[1] Although these independent systems each have their own governing bodies and law enforcement agencies, shared areas of legitimate governmental interests, such as combating drug-trafficking, result in overlapping and concurrent jurisdiction where the federal and state governments act independently or even jointly to address these mutual problems. This discussion will focus on the use of electronic surveillance as an investigative technique used in the federal system and will not discuss the systems of the various states and their laws.

As practiced in the federal system, electronic surveillance (commonly referred to as "wiretapping") is one of the most effective law enforcement tools for investigating many types of criminal enterprises. In the United States, electronic surveillance has been used successfully to prosecute traditional organized crime (the American mafia or La Costra Nostra), large drug-trafficking organizations, violent street gangs, and criminals involved in various types of public corruption and fraud. In a recent, for example, electronic surveillance was used successfully to uncover a fraud scheme that victimized the McDonald's restaurant chain and its customers. McDonald's was sponsoring games of chance for its customers, which involved prizes of up to one million dollars. The defendants, who were responsible for running the contests for McDonald's, pre-selected the winners in exchange for a portion of the prize money. In this case, the electronic surveillance led to the arrests of several persons who are currently awaiting trial.

Since 1990, the number of federal investigations using electronic surveillance has increased dramatically, and that trend is expected to continue. In 1990, federal law enforcement agencies submitted a total of 791 electronic surveillance requests to the Department of Justice for approval. Between October 1, 2000, and September 20, 2001, the federal agencies submitted over 1,700 electronic surveillance requests. Over the past ten years, there has been not only an increase in the number of electronic surveillance requests, but also a growing number of investigations that have multi-jurisdictional and international components, particularly in the area of drug trafficking and alien smuggling,

* Chief, Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, United States Department of Justice

** As a consequence of the terrorist attacks in the U.S.A. on 11 September 2001, Ms. Wuslich was unable to attend the 119th International Training Course. Copies of the two lectures Ms. Wuslich had prepared were distributed to all of the participants.

[1] The federal system includes federal law affecting all 50 states, as well as the territories of the United States Virgin Islands, the District of Columbia, Puerto Rico, Guam, and the Northern Mariana Islands. The state system is comprised of the 50 state governments.

where American traffickers and smugglers have co-conspirators overseas and in multiple states within the United States. Crime, once primarily a local concern, has gone global. The proliferation of the Internet and the use of hand-held communications devices, such as cellular telephones and two-way pagers, has increased a criminal's mobility, expanded the reach of his or her criminal enterprise, and shortened the time necessary to plan and execute even the most complex crimes.

While electronic surveillance is a very valuable technique, and has yielded tremendous results in some significant investigations, it is also a very intrusive one that implicates privacy rights protected under the United States Constitution, particularly the Fourth Amendment protection against unreasonable searches and seizures. For that reason, significant legal and policy restrictions have been placed on the use of electronic surveillance in the United States, mostly imposed by Congress and some imposed by the courts. These restrictions are designed to balance the needs of law enforcement to fight crime against the right of citizens to be free of overbroad or unnecessary government intrusion into individual privacy.

II. LEGAL REQUIREMENTS

A. Background Of Title III

In 1968, the United States Congress enacted the federal electronic surveillance statutes, which are often referred to as Title III of the Omnibus Crime Control And Safe Streets Act of 1968 (hereinafter, "Title III").[2] Congress enacted Title III in response to several United States Supreme Court decisions recognizing the applicability of constitutional protections to an individual's communications, and because it wanted to regulate the use of electronic surveillance by law enforcement and private citizens, resolve conflicts in the law, set a federal standard by which electronic surveillance would be conducted and, most importantly, to combat organized crime.[3] In 1968, organized crime (La Cosa Nostra) was seen as a plague on American society, and was credited with controlling various criminal enterprises, such as drug-trafficking, gambling, loansharking, and prostitution, and corruptly influencing legitimate businesses, labor unions, and the political process.

While Congress wanted to give law enforcement an effective tool to eradicate organized crime, it also wanted to tightly control the use of electronic surveillance to avoid abuse of the technique and to protect individual privacy, as constitutionally required. To accomplish these conflicting, yet important goals, Congress: 1) enacted a two-step approval process requiring Executive and Judicial Branch concurrence for two of three types of communications a law enforcement officer is permitted to intercept; 2) limited the types of crimes for which electronic surveillance can be authorized; 3) restricted electronic surveillance to thirty-day intervals and; 4) required the government to submit an affidavit to the authorizing authorities which would justify the electronic surveillance and outline how the government would comply with the statutory requirements. Each of these fundamental requirements and their related statutory components will be discussed, in turn.

[2] 18 U.S.C. §§2510–2522.

[3] United States Senate Report No. 1097, 90th Congress, 2nd Session, 1968.

B. The Approval Process

When law enforcement agents of a government investigative agency want to conduct a wiretap over a telephone or install listening devices in a location, they must obtain approval from two entities.[4] First, they must obtain approval from a statutorily specified high-level official at the Department of Justice, who must concur in the need for the proposed interception and find that it meets all of the statutory and constitutional requirements. The Department official does not authorize the interception, but instead authorizes the government agents to apply to the appropriate federal court for an order authorizing the interception. Second, the agents must then obtain such an order from a federal district court judge. Congress enacted the provision requiring Justice Department approval because it believed that centralized review by the Department would promote national uniformity in the way electronic surveillance was conducted, and because Congress wanted to hold a politically accountable official responsible for any abuses that might occur.

With regard to approval by a judge, Congress enacted this provision in accordance with constitutional principles that require a detached and neutral authority to review and authorize certain types of law enforcement action directed against the citizenry.

Unless the government has obtained both approvals, and in the correct order, it cannot conduct the electronic surveillance.[5] If the government fails to get both approvals, but conducts the electronic surveillance, the evidence must be suppressed and the government will not be allowed to use that evidence, or any derivative evidence, at trial.[6]

The approval process at the Justice Department usually takes a few days and involves the following process. When a federal investigative agency and the United States Attorney's Office in the location where the crime is being committed[7] is ready to conduct electronic surveillance in an investigation, it submits an affidavit as part of its application[8] to conduct surveillance to the Electronic Surveillance Unit, which is part of the Justice Department's Criminal Division. An attorney in that Unit reviews the affidavit for legal sufficiency. If the affidavit meets the statutory requirements, it is forwarded to the appropriate high-level official for review along with a recommendation that the request be approved. If the official agrees that the affidavit is legally sufficient, he or she will grant the request. At that point, the government may submit the application and approved affidavit to a judge, who may grant or deny the request to conduct the surveillance. If the judge grants the request, he or she will issue an interception order, which allows the law enforcement agency to conduct surveillance over a particular telephone/facility or within a particular location for a thirty-day period. Most judges will issue

[4] 18 U.S.C. §2516(1).

[5] United States v. Reyna, 218 F.3d 1108 (9th Cir. 2000).

[6] United States v. Chavez, 416 U.S. 562 (1974).

[7] Many times throughout this paper, the term "government" is used to refer collectively to the federal investigative agencies and the United States Attorney's Offices, or their representatives.

[8] 18 U.S.C. §2518(1); United States v. Williams, 124 F.3d 411 (3d Cir. 1997)(The procedure of submitting a sworn affidavit by a law enforcement officer, which is attached to prosecutor's application, is sufficient.).

the order the same day they receive the request from the government.

It should be noted that when Title III was amended in 1986 to specifically provide for the interception of electronic communications, which are communications that occur, *inter alia*, over a paging device, a computer, or a facsimile machine, Congress required only approval by a judge, without the predicate Department review and approval.[9] Congress did not consider the interception of these communications to involve the same level of intrusion into a person's privacy as the interception of a person's telephone calls or private conversations. Nevertheless, by agreement between Congress and the Justice Department, internal Department policies require review and approval prior to applying to the court for an order authorizing the interception of electronic communications over computers, facsimile machines, and two-way paging devices.

The requirements for the government's affidavit in support of the electronic surveillance application to the court are discussed below.

C. The Affidavit

1. Sworn to by a Law Enforcement Officer

Like a traditional search warrant under longstanding United States law, Title III requires the application to be made by a federal law enforcement officer, who has investigative and arrest powers for the crimes under investigation and who swears to the facts and statements set forth in the affidavit.[10] As a matter of policy, the Department of Justice limits the number of federal agencies which can conduct electronic surveillance. The Department does this to ensure that only the agencies with the most expertise, resources, and experience can conduct electronic surveillance as part of their investigations. Those agencies that are not historically approved to conduct electronic surveillance can do so only when partnered with an approved agency, usually the Federal Bureau of Investigation ("FBI"), where both agencies have jurisdiction over the crimes under investigation.

2. Identifying the Persons Committing the Crimes

Title III requires the government to identify by name, if it can, the persons who are committing the crimes under investigation and who are expected to be intercepted over the specified telephone or within the location.[11] This provision serves two purposes. First, it requires that the government determine if the persons identified in the affidavit have been the subject of prior electronic surveillance.[12] If they have, the government must include in the affidavit all of the information about such prior surveillance. One of the reasons this information is required is so that the judge may determine if the government is being overzealous in its investigation of these individuals, such as could be the case if numerous, prior court-authorized interceptions had failed to produce any evidence of criminal involvement by the targets. In such a situation, the judge may require the government to justify the request.[13] Second, at the conclusion of the

[9] 18 U.S.C. §2516(3); The Electronic Communications Privacy Act of 1986, United States Senate Report No. 541, 99th Congress, 2nd Session, 1986.

[10] 18 U.S.C. §2518(1).

[11] 18 U.S.C. §2518(1)(b)(iv).

[12] 18 U.S.C. §2518(1)(e).

[13] 18 U.S.C. §2518(2).

investigation, the government must give notice to the persons named in the affidavit that they were intercepted so that these persons can prepare their defense if charges are brought, or otherwise challenge the legality of the surveillance.[14]

3. Identifying the Facility or the Location and the Type of Communication

Next, under Title III, and in compliance with the Fourth Amendment, the government must identify, with particularity, the telephone facility or location that will be the subject of the electronic surveillance, and the type of communication that will be intercepted, i.e., telephone conversations (wire communications), face-to-face conversations (oral communications), or computer transmissions, pager data, or facsimile transmissions (electronic communications).[15] This requirement ensures that the law enforcement officer who is conducting the surveillance knows what facility or location—and what kind of communications—he or she is allowed to intercept. This prevents the law enforcement officer from conducting an open-ended or overly broad search, targeting any telephone or location used by a subject (except for "roving" interceptions, discussed *infra*). However, once the government has established that a particular telephone or a location is being used to facilitate criminal activity, the court's order generally provides that the government can intercept the criminal-related communications of anyone who may use that telephone or location, and not just those persons named originally in the court order.[16]

The exception to the particularity requirement is the "roving" provision of Title III. Under Title 18, United States Code, Section 2518(11), the government can obtain a court order for a 30-day period to intercept communications over any telephone/facility or within any location that a specific subject may be using to commit the crimes. For example, drug traffickers often use a series of different cellular telephones to carry out their criminal activities, and will often use a telephone for only a few days in order to prevent law enforcement detection of their crimes. By the time the government has identified the telephone the subject is using and obtains the requisite approvals, the subject may no longer be using it. The roving provision allows the government to intercept communications over any telephone the subject may obtain and use during the 30-day period as long as the government can show that the subject's behavior has the effect of thwarting its ability to intercept his or her calls, and that the subject has a pattern of using multiple telephones to conduct his or her criminal activity. With respect to a location, the government must show that it is unable to specify in advance to the reviewing court where the subject and his or her co-conspirators will be meeting to conduct their criminal activity. In one case, the government obtained a court order to intercept communications of Mafia members who were planning to conduct a ceremony to induct new members into the crime family.[17] The government's confidential informant, who would be present at the ceremony, would not learn of the meeting location until a few hours before the ceremony was to take place. A more recent example involved a public corruption case, wherein the subject of

[14] 18 U.S.C. §2518(8)(d).

[15] 18 U.S.C. §2518(1)(b)(ii), (iii).

[16] United States v. Kahn, 415 U.S. 143 (1974).

[17] United States v. Ferrara 771 F. Supp. 1266 (D. Mass. 1991).

the investigation scheduled meetings with his co-conspirators at the last minute to make bribe payments, and had not been seen meeting with them at the same location twice.

After the government obtains a court order to conduct roving interceptions over different telephones or within different locations, the government may only intercept the communications of the subjects identified in the affidavit as the users of the telephones or locations, and subjects in communication with them. If other subjects of the investigation are using the telephones or locations, without the named subjects also participating in the communication, the government cannot intercept those communications, even if they are criminal in nature.[18]

4. Listing the Crimes under Investigation

Title III allows for electronic surveillance only when the government is investigating one of several crimes listed in the statute. Congress decided that electronic surveillance should be used to investigate only the most serious types of offenses. If the government wants to wiretap a telephone (wire communications) or install listening devices in a location to capture face-to-face communications (oral communications), the government must be investigating one of the enumerated offenses listed in Title III.[19] If the government wants to intercept communications over a computer, a pager, or a facsimile machine (electronic communications), the government only needs to be investigating a federal felony offense, which again recognizes Congress's view that electronic communications warrant lesser protection than required for wire and oral communications.[20] By requiring the government to identify which crimes are under investigation, the statute again ensures that the electronic surveillance will not be overly broad or unnecessarily intrusive.

5. Establishing Probable Cause

In accordance with the Fourth Amendment, Title III requires the government to outline the facts that show a particular telephone or location is being used to facilitate the commission of criminal acts.[21] There are several ways the government can do that. For example, the government may have a confidential informant or an undercover law enforcement agent who can engage the subject in a discussion of criminal activity during a call over the telephone or during a meeting within the location. The drug dealer may instruct the informant to call the drug dealer on a particular telephone when the informant wants to buy cocaine. Thereafter, the informant calls the drug dealer at that telephone. During the call, the informant asks to buy a quantity of cocaine and the dealer agrees to make the sale at a nearby parking lot. The informant travels to the parking lot, meets the dealer, and buys the cocaine. It is clear from that chain of events that the drug dealer used the telephone to facilitate his or her drug business.

6. Establishing the Need for the Electronic Surveillance

Because electronic surveillance is so intrusive, the government must show why it needs to conduct electronic surveillance to gather the evidence necessary to prosecute the subjects.[22] Specifically, the government must state

[18] United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996); United States v. Jackson, 207 F.3d 910 (7th Cir. 2000).

[19] 18 U.S.C. §2516(1).

[20] 18 U.S.C. §2516(3).

[21] 18 U.S.C. §2518(1)(b).

[22] 18 U.S.C. §2518(1)(b).

what other investigative procedures have been tried, and if not, why they would be unlikely to succeed or would be to dangerous to use. These other procedures include physical surveillance of the subjects, search warrants executed at locations or residences known to be used by the subjects, interviews of the subjects or their associates, the use of a grand jury to investigate the subjects, examination of telephone records for their telephones, and seizures of contraband. If the government has not performed each of these investigative techniques, it must explain why it cannot do so, or, even if it did, why using the technique would not be sufficient in and of itself to meet the goals of the investigation. For example, the government may have conducted physical surveillance of the subjects, but the subjects observed the surveillance agents and stopped their criminal activities, or the subjects routinely engage in counter-surveillance maneuvers, which create a danger to the police officers or others, or the subjects live or travel in an area that makes such surveillance difficult. In one case, the FBI was investigating a cocaine conspiracy in a small town. One day, FBI agents were conducting physical surveillance, and the mayor of the town began to follow the agents. The mayor escalated his pursuit of the agents and forced the agents to drive out of town. The FBI learned later that the mayor chased the agents because they were suspicious strangers. Moreover, the government may have used confidential informants or undercover agents at one time in their case producing some evidence supporting the investigation, but the subjects discovered their identities and to continue to use them would compromise their safety. The government may also have seized contraband from a vehicle during a search, but the driver of the vehicle refuses to cooperate or was only privy to limited information about the person to whom he was delivering the drugs.

7. Prior Electronic Surveillance

Title III requires that the government set forth in the affidavit whether any of the subjects, facilities, or locations have been the subject of prior surveillance.[23] The government is required to give a full and complete statement of any prior electronic surveillance orders. That statement includes the dates of the prior orders, the names of the subjects of the investigation in those orders, and what facilities or locations were the subject of the electronic surveillance. As explained previously, one of the purposes of this requirement is for the judge to determine if the government is being overzealous in its investigation of these individuals. These checks must be done by all of the investigative agencies that may have conducted electronic surveillance of the subjects, and not just the agency making the instant request.

8. Statement of Time

Under Title III, the government can only conduct electronic surveillance for a period of up to 30 days, and the affidavit must contain a statement to this effect.[24] If the government has not met its investigative goals during the first 30 days of interceptions, the government may seek approval from the Department of Justice and the judge to conduct interceptions for another 30-day period. Each time the government applies for an extension order, it must describe the evidence derived from the wiretap and demonstrate a continuing investigative need to intercept the communications.[25] There is no statutory limit on the number of times the government can seek to

[23] 18 U.S.C. §2518(1)(e).

[24] 18 U.S.C. §2518(1)(d), (5).

[25] 18 U.S.C. §2518(1)(f).

extend the electronic surveillance. As long as the government meets the statutory requirements each time, and the judge so permits, the government may continue to conduct surveillance. The average electronic surveillance investigation is conducted for approximately four months. It is the exceptional electronic surveillance investigation that lasts for a year or longer.

9. Minimization

Title III requires that the government minimize the interception of communications not related to the crimes under investigation.[26] This means that the government is required to terminate the interception of the communication when the communication does not concern the criminal matters under investigation or any other type of criminal activity.[27] For example, if a law enforcement officer is listening to a telephone call and the subjects are not talking about their identified criminal activities or any other crime, the officer must turn off the monitoring equipment. After a reasonable interval, the officer can turn the equipment back on to determine if the call has become criminal in nature. If the subjects are now talking about their crimes, the officer can listen to and record the call. When monitoring a call, the officer may have to turn the equipment off and on several times. To determine if the government lawfully minimized the communications, the courts consider the following factors: 1) the number of co-conspirators; 2) the complexity of the crimes being committed; 3) the size and longevity of the criminal enterprise; 4) the actions taken by the monitoring officers to minimize the communications and whether they showed a high regard for the subjects' privacy; 5) the use of coded language by the subjects; 6) whether the telephone or the location is the center of the criminal activity; 7) judicial review and approval of the minimization efforts; and 8) whether the monitoring agents were adequately instructed on the proper minimization techniques.[28]

There is a statutory exception to the requirement to minimize communications as they are occurring. If the subjects are conversing in a foreign language or in a code that the law enforcement officers do not understand, and the government does not have translators available to translate and minimize the communications as they are occurring, Title III allows the government to record the conversations in their entirety and minimize the conversations later.[29] This procedure is called "after-the-fact minimization." The key to after-the-fact minimization is that the process used must protect the subject's privacy interests to approximately the same extent as would contemporaneous minimization. To achieve this result, translators are told to translate only the portions of the recorded communications that seem relevant to the crimes under investigation. The translators then give only the relevant portions of the communications to the law enforcement

[26] 18 U.S.C. §2518(5).

[27] Congress anticipated that communications about crimes that were not identified in the order might be intercepted during a lawfully conducted wiretap. The government may intercept those communications, and disseminate those communications to law enforcement officers for further investigation. If the government wants to use those communications in subsequent court proceedings, it may do so if it obtains an order under 18 U.S.C. §2517(5).

[28] United States v. Parks, 1997 WL 136761 (N.D. Ill.).

[29] 18 U.S.C. §2518(5).

officers investigating the case. The non-relevant parts of the communications are placed under seal with the court and are not reviewed by the law enforcement officers.[30]

While not explicitly provided for in Title III, there are other instances when the government cannot minimize the interception of communications as they are occurring, but must intercept, record, and review the entire communication to determine its relevance to the investigation.[31] One instance involves electronic communications over facsimile machines, computers, and pager devices, and another instance involves voice-mail left on a telephone system. Given the nature of the communication and the way it is transmitted, the government must intercept the whole communication and use the after-the-fact minimization procedures, disclosing and using only those communications that are relevant to the investigation, and sealing the information that is not relevant.

III. EMERGENCY INTERCEPTIONS

Congress, in recognizing that there are emergency circumstances under which the normal approval processes must be circumvented, enacted a provision by which law enforcement may conduct electronic surveillance without first obtaining a court order. A discussion of that provision follows.

With the approval of a highly-placed Department of Justice official, Title III allows the government to conduct interceptions over a particular facility or within a location without first obtaining a court order when: 1) there is an imminent threat of death or serious bodily harm to an individual; 2) there is a threat to national security; or 3) events characteristic of organized crime are about to occur, and interceptions must begin before a court order can, with due diligence, be obtained in order to prevent the harm, forestall the threat, or capture evidence of the organized crime activity.[32] To illustrate these principles and the process involved, consider the following example. The FBI receives information that several armed gunmen have robbed a bank and have taken hostages. Upon arrival at the scene, the FBI observes through the windows of the bank three masked, armed gunmen and four hostages, bound and blindfolded. The FBI also sees that one of the gunmen is talking on a cellular telephone, leading them to believe that the gunman is conversing with co-conspirators. The FBI hostage negotiator reports that the gunmen are making demands for money and safe passage from the bank and out of the country, and that they want to take one of the hostages with them. The gunmen have given the FBI four hours to comply with their demands. At this stage, the FBI identifies the telephone that the gunman is using[33] and decides to contact the telephone company to obtain records for the telephone that will show what telephone numbers are being called from the gunman's telephone.[34] An analysis of the calling records reveals that the gunman's telephone is being used to call a telephone that is registered to the person who also appears as the registered owner

[30] United States v. David, 940 F.2d 722 (1st Cir. 1991); United States v. Padilla-Pena, 129 F.3d 457 (8th Cir. 1997).

[31] United States v. Tutino, 883 F.2d 1125 (2nd Cir. 1989).

[32] 18 U.S.C. §2518(7).

[33] When turned on, a cellular telephone emits certain signals. Law enforcement can capture these signals through specialized equipment and identify the telephone.

[34] 18 U.S.C. §2703(c)(1)(C).

of a suspected getaway car parked outside of the bank. (A check of motor vehicle records reveals that the name and address information listed for this person is fictitious.) Unable to proceed further, the FBI decides to seek emergency authorization to intercept communications over the telephone used by the gunman. The FBI hopes to obtain information that will help to resolve the situation peacefully, as well to gather evidence about the identities of the gunmen and any of their co-conspirators. To begin the process, the FBI contacts a federal prosecutor in the appropriate United States Attorney's Office, who contacts the Criminal Division of the Justice Department and talks to one of the lawyers in the Electronic Surveillance Unit. That lawyer coordinates the approval process orally within the Department and with the FBI, and one hour later, the Attorney General personally grants the head of the FBI permission to decide whether an emergency situation exists as defined by the statute and, if so, to intercept calls over the gunman's phone.

From the time the Attorney General authorizes the interception, the prosecutor has 48 hours to obtain a court order approving the emergency interception. The court order must be based on a written affidavit that is sworn to by a law enforcement officer and sets forth the facts known at the time the emergency was authorized by the Attorney General. If the prosecutor fails to obtain the order within the 48-hour time period, the intercepted telephone calls and any evidence derived from the electronic surveillance must be suppressed. If the emergency situation has not been resolved within the 48-hour period, and the government wants to continue to intercept calls over the telephone, the government must submit an affidavit to the Department of Justice for approval to seek a court order to do so. It is important to note that all of the requirements of Title III apply to emergency situations. The government must have probable cause to believe that communications about a crime listed in the statute will be intercepted over the telephone/facility, or within the location, and that alternative investigative techniques will not suffice to prove the crimes or forestall the danger or threat.

IV. POST-INTERCEPTION REQUIREMENTS

A. The Sealing Requirement

Title III requires that when the government has concluded its electronic surveillance investigation, it must take the original recordings of the communications and place them under seal with the court.[35] The sealing requirement ensures the integrity of the recordings and enables their use at trial. If the government fails to seal the recordings in a timely manner, the court may prohibit their use at trial.[36] Because sealing is only required at the end of the electronic surveillance investigation, the government could continue the interceptions for over a year without having to seal the recordings. However, the Justice Department recommends sealing the recordings every 30 days to ensure the continuing evidentiary value of the recordings.

B. The Notice Requirement

Within 90 days of the conclusion of the electronic surveillance investigation, the government must notify the named subjects that they were the targets of an electronic surveillance investigation.[37]

[35] 18 U.S.C. §2518(8)(a).

[36] United States v. Ojeda-Rios, 495 U.S. 257 (1990).

[37] 18 U.S.C. §2518(8)(d).

This provision gives the subjects the opportunity to challenge the electronic surveillance evidence. If, at the end of the 90-day period, the government is still investigating the subjects, it may seek to postpone the notice for another 90 days, or until further order of the court.

V. ACTIVITY NOT COVERED BY TITLE III

A. Consensual Recordings

Title III, by its terms, does not apply to the interception and recording of telephone calls, face-to-face conversations, or computer or pager transmissions that are made by a law enforcement officer, a confidential informant, or a private citizen, when that person is a participant in the communication.[38] The legal rationale is that a person does not have a reasonable expectation to believe that the person with whom he or she communicates will keep his or her confidence.[39] Therefore, the government does not have to obtain Department of Justice approval or a court order before an undercover government agent or a confidential informant may record a telephone call or a conversation with the subject of a criminal investigation. Additionally, a private citizen may record his or her communications with others as long as he or she is not recording the communications for the purpose of committing a crime or a tortious act. An example of a criminal or tortious act would be that the communication was recorded in order to blackmail someone.

Consensual recordings of a person's communications are strong evidence of that person's criminal culpability, and they are commonly used to establish that a person is using a location or a telephone to facilitate the commission of a crime. Therefore, consensual recordings are a very valuable technique for law enforcement to use when a government agent or an informant has gained the trust of someone suspected of criminal wrongdoing.

B. Prison Monitoring

Under Title III, the government may monitor inmate calls over prison telephone lines without obtaining Department of Justice approval or a court order. Specifically, 18 U.S.C. §2510(5)(a) allows the recording of telephone conversations of inmates by prison officials to ensure the safe and orderly administration of the prison. If, however, the government wants to investigate the criminal activities of a particular inmate involving crimes with persons outside of the prison system, the Department of Justice, as a matter of policy, requires the government to obtain its approval and a court order to conduct the electronic surveillance.

C. Video Surveillance

Another common investigative technique that is not proscribed by Title III involves the use of closed-circuit, hidden cameras to record a subject's criminal conduct. Although Title III does not regulate or prohibit the use of video surveillance, several court opinions have circumscribed its use.[40] In accordance

[38] 18 U.S.C. §2511(2)(c), (d).

[39] Lopez v. United States, 373 U.S. 427 (1963); Hoffa v. United States, 385 U.S. 293 (1966); United States v. White, 401 U.S. 745 (1971).

[40] United States v. Falls, 34 F.3d 674 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Biasucci, 786 F2d 504 (2d Cir. 1986); United States v. Torres, 751 F.2d 875 (7th Cir. 1984); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990).

with these opinions, the government must obtain a court order to conduct video surveillance in any area where the subject has a reasonable expectation of privacy. The court order must be based on a warrant sworn to by a law enforcement officer that establishes reason to believe that the subject(s) will be engaged in criminal conduct in the location that will be videotaped. Video surveillance is often used in drug-trafficking cases where the government believes that contraband will be stored at, or delivered to, a particular location, and it wants to identify the persons involved in the drug activity.

VI. SUPPRESSION OF TITLE III EVIDENCE

Title III contains a statutory suppression rule that provides that the government cannot use electronic surveillance evidence or any evidence derived from the surveillance in a court proceeding if: 1) the communications were intercepted unlawfully; 2) the court order approving the electronic surveillance was insufficient on its face; or 3) the interceptions were not conducted in accordance with the order.[41] Because the court order authorizing the electronic surveillance is based on an *ex parte*, *in camera* showing of facts by the government, the judge who authorized the wiretap, when presented with a defense motion to suppress, may reconsider the original facts and decide that suppression is warranted. A court hearing to determine if the evidence will be suppressed is triggered by a motion to suppress the evidence by the defendant's attorney.[42]

Title III evidence has been suppressed because the government failed to establish an investigative necessity for the electronic surveillance.[43] Title III evidence has also been suppressed because the government failed to determine if the subjects had been the subject of prior electronic surveillance,[44] and when the government failed to obtain Department of Justice approval before it obtained the court order for the electronic surveillance.[45]

Because of the safeguards placed on the government's use of electronic surveillance, Title III evidence is rarely suppressed.

VII. CONCLUSION

While Title III limits government conduct with regard to the use of electronic surveillance, this law has provided reasonable guidelines well understood by investigative agents and prosecutors, and these guidelines ensure that the interceptions conducted pursuant to court orders will result in the successful prosecutions of those who communications are intercepted.

[41] 18 U.S.C. §2515; United States v. Ruggiero, 824 F. Supp. 379 (S.D.N.Y. 1993).

[42] 18 U.S.C. §2518(10)(a).

[43] United States v. Aileman, 986 F. Supp. 1228 (N.D. Cal. 1997).

[44] United States v. Luong, No. CR-94-0094 MHP (N.D. Cal. 7/14/98) (unpublished).

[45] Reyna, supra.