Interception of Communications in Exigent Circumstances: The Fourth Amendment, Federal Legislation, and the United States Department of Justice

Clifford S. Fishman
The Catholic University of America, Columbus School of Law
ARTICLES

INTERCEPTION OF COMMUNICATIONS IN EXIGENT CIRCUMSTANCES: THE FOURTH AMENDMENT, FEDERAL LEGISLATION, AND THE UNITED STATES DEPARTMENT OF JUSTICE

Clifford S. Fishman*

TABLE OF CONTENTS

I. THE FOURTH AMENDMENT AND WARRANTLESS INTERCEPTION OF COMMUNICATIONS ...................... 10
   A. The Warrant Requirement ............................ 10
   B. The “Exigent Circumstances” Doctrine ........... 13
      1. Life-Threatening Exigencies .................... 13
      2. Hot Pursuit ........................................... 13
      3. Preserving Evidence from Destruction...... 14

* Professor of Law, The Catholic University of America School of Law. A.B., University of Rochester, 1966; J.D., Columbia University, 1969. Between 1969 and 1977, Professor Fishman served as an Assistant District Attorney in the New York County District Attorney’s Office and as Executive Assistant District Attorney in New York City’s Special Narcotics Prosecutor’s Office, during which he drafted and supervised the execution of 35 wiretapping and eavesdropping orders. For additional details, see infra note 397. From 1984 to 1986, Professor Fishman served as a consultant on electronic surveillance for the President’s Commission on Organized Crime.
C. Applicability of the "Exigent Circumstances" Doctrine to Electronic Surveillance................. 19

II. **TITLE III: PREREQUISITES TO COURT-ORDERED SURVEILLANCE** .................................................... 23
A. Application and Order .................................. 25
1. In general............................................ 25
2. Particularity........................................ 27
   a. "Specific offense"........................... 29
   b. "Specific person"............................ 29
B. Execution of an Intercept Order: the Minimization Provision ........................................... 33

III. **THE "EMERGENCY SURVEILLANCE" PROVISION** ........ 35
A. Interpretation and Application of the Requirements .............................................. 35
1. Grounds for an order.............................. 36
2. "Emergency situation"............................ 37
3. Factual settings in which emergency surveillance is permitted .................................... 37
   a. The immediate danger clause ............ 38
   b. The organized crime clause .............. 39
4. Pre-interception authorization ................ 40
5. Post-interception authorization ............ 40
B. Justice Department Policies and Practices ...... 41
   1. The application authorization process .... 41
   2. Emergency surveillance ..................... 46

IV. **THE ROVING INTERCEPT PROVISION** ...................... 48
A. Application and Order: Additional Requirements ............................................ 49
   1. Authorization for application................ 50
   2. Identity of intended interceptee ............ 50
   3. Showing of need ................................ 52
   4. Description of Communications ............... 56
B. Implementation of Roving Intercept Orders .... 58
   1. Knowledge of facilities or location ....... 58
   2. Anticipatory installation of devices ....... 58
   3. Minimization .................................. 63
   4. Telephone company cooperation ............ 64
C. Constitutionality of the Roving Intercept Provision ................................................... 65
   1. In general...................................... 65
In *The Day of the Jackal*, Frederick Forsyth's 1971 novel, French authorities learned that a professional assassin of unknown identity had been hired by disgruntled former army officers to assassinate President Charles DeGaulle. The Minister of the Interior called the heads of all French law enforcement agencies to an emergency meeting. These officials quickly realized that until they could discover who the killer was, there was little they could do to frustrate his plan. The President had already refused to alter his schedule or behavior; to do so in the face of a death-threat, he insisted, would be beneath his dignity and an affront to the nation's.

A detective, praised by his agency head as the best in France, was summoned and instructed to identify and apprehend the assassin. He was given extraordinary authority to accomplish this task, and he was told to report daily to the assembled agency heads. The detective quickly learned of the assassin's false identities. On several occasions the Jackal's capture seemed certain, yet each time the quarry managed to slip out of the trap.

Eventually, the detective suggested that someone might be leaking information about the investigation. This possibility was spurned by

---

the agency heads as a puerile attempt to excuse failure. A day or two later, the detective confronted them, insisting that someone who had been attending these secret daily briefings was the source of the leak.

When challenged to substantiate this accusation, the detective played a tape recording. The officials heard a woman place a phone call and repeat information about the assassin's location that the detective had reported only one day earlier. When the tape ended, the Deputy Chief of the Presidential Security Corps rose, ashen-faced, admitted that the woman was a "friend" who was "staying with me at the present time," and stumbled from the room.

It is easy to imagine the admiration and gratitude with which the remaining chiefs then regarded the detective. (It helped that the Deputy Chief had not been particularly popular with his colleagues.) Then the Minister asked the detective how he knew to tap the Deputy Chief's home telephone. The detective responded, "I didn't, so last night I tapped all your telephones."2

The sudden change in mood presumably precipitated by this announcement mirrors, in many ways, the prevailing American attitudes about electronic surveillance. We expect the police to act promptly and effectively to combat crime, but we insist that in doing so they respect and protect the right to privacy that is guaranteed by the Fourth Amendment3 and enshrined in our values as an essential component of individual freedom and dignity. Wiretapping and eavesdropping are among the most effective investigative techniques available to combat crime. To many observers, however, surreptitious monitoring of private conversations conjures images of Nazi Germany, the Soviet Union, and fictional equivalents.4 To strike the

---

2 Id. at 347.
3 "Fourth Amendment" is capitalized throughout this Article, despite the dictates of A Uniform System of Citation, Rule 8 (14th ed. 1986), at Professor Fishman's request.
4 The Watergate scandal of the early 1970s should suffice to destroy any illusions that the United States is somehow inherently immune from the misuse of these techniques. The scandal began in 1971 when individuals working for the re-election of President Nixon bugged the Democratic Party's offices in Washington, D.C. The President and his closest advisors conspired to cover-up the involvement of their political associates. At the same time, Nixon had been secretly recording many of his private conversations—including conversations proving his own participation in the conspiracy to obstruct the investigation into the Watergate
proper balance, to permit the police to tap and bug under appropriate circumstances, while protecting the right to privacy against police overreaching, has been one of the greatest challenges our legal system has confronted in the past half-century.\textsuperscript{5}

For the last twenty years, law enforcement use of wiretapping and eavesdropping has been regulated by Title III of the Omnibus Crime Control and Safe Streets Act of 1968.\textsuperscript{6} Congress enacted Title III

\begin{footnotes}
\item[5] In 1928, the Supreme Court held that the Fourth Amendment was inapplicable to wiretapping unless government officials had physically invaded the defendant's premises. \textit{Olmstead v. United States}, 277 U.S. 438, 466 (1928). Congress eventually responded by enacting section 605 of the Federal Communications Act of 1934, ch. 652, § 605, 48 Stat. 1103 (1934) (current version at 47 U.S.C. § 605 (1982 & Supp. III 1985)), which provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish [any aspect of the communication]." The Supreme Court, while standing by \textit{Olmstead}, subsequently held that § 605 applied to intrastate as well as interstate communications, \textit{Weiss v. United States}, 308 U.S. 321, 329 (1939), and prohibited wiretapping by state and federal officers as well as by private persons, \textit{Benanti v. United States}, 355 U.S. 96, 100 (1957) (state officers); \textit{Nardone v. United States}, 302 U.S. 379, 383 (1937) (federal officers), \textit{appeal after remand and trial}, 308 U.S. 338 (1939).

The Court also applied the \textit{Olmstead} rule limiting Fourth Amendment protection to physical trespass in several opinions relating to bugging (electronic eavesdropping on face-to-face conversations). In \textit{Goldman v. United States}, 316 U.S. 129 (1942), federal agents overheard conversations between defendants Goldman and Schuman by pressing a listening device against the wall adjoining Shulman's office. Since there had been no physical trespass into Schuman's premises, the Court reasoned that no search had occurred. \textit{Id.} at 134-35. In \textit{Silverman v. United States}, 365 U.S. 505 (1961), however, the Court held that an illegal search \textit{had} occurred when police drove a microphone several inches into a party wall of the suspect's house. In \textit{Clinton v. Virginia}, 377 U.S. 158 (1964) (facts related in \textit{Clinton v. Virginia}, 204 Va. 275, 130 S.E.2d 437 (1963)), the Court arrived at the same conclusion where the microphone's penetration was only thumbtack deep.

Ultimately, the Supreme Court abandoned the trespass doctrine of \textit{Olmstead} and \textit{Goldman}. In \textit{Katz v. United States}, 387 U.S. 347, 353 (1967), the Court held that the surreptitious interception of private communications constituted a search under the Fourth Amendment regardless of whether investigators had intruded into any constitutionally protected "area." Soon thereafter, Congress enacted the legislation discussed at infra note 6.

with at least four specific goals in mind. First, in permitting investigators to obtain court authorization to wiretap or eavesdrop, it sought to provide law enforcement officials with a much-needed weapon in their fight against crime, particularly organized crime. Second, it sought to safeguard the privacy of wire and oral communications. Third, Congress endeavored to satisfy the procedural and substantive requirements previously enunciated by the United States Supreme Court in *Berger v. New York* and *Katz v. United

*Politics of 'Law and Order', 67 Mich. L. Rev. 455 (1969); Spritzer, *Electronic Surveillance by Leave of the Magistrate: The Case in Opposition*, 118 U. Pa. L. Rev. 169 (1969). Although the controversy has dampened somewhat, it has not abated completely. When Congress enacted Title III, supra, it also created a Commission to study existing electronic surveillance law, see Title III, supra, § 804, 82 Stat. 197, 223 (1968) which, after extensive hearings and studies, in 1976 issued a lengthy report. See *National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance, Electronic Surveillance Report* (1976) [hereinafter NWC Report]. Although the Commission endorsed Title III, a substantial number of commissioners concluded that Title III had failed to serve the purposes it was intended to further, and called for its repeal. *Id.* at 177, 179-92 (minority report of Sen. Abourezk, Reps. Kastenmeier and Seilberling, and Prof. Westin); *id.* at 213-17 (separate statement of Prof. Westin). See also H. SCHWARTZ, TAPS, BUGS, AND FOOLING THE PEOPLE (1977) (criticism of Title III and the way it has been used); Margolis, *Human Rights Commentator*, 50 Conn. B.J. 559 (1976) (also criticizing Title III). Many may agree with one district court judge that “[w]e are becoming a society that must exist in constant hazard from official snooping,” and that “[w]hatever incidental good flows from this invasion of privacy is submerged by the growing appearance of police surveillance so typical of totalitarian states.” United States v. Kline, 366 F. Supp. 994, 996-97 (D.D.C. 1973) (Gesell, J.).

*Title III, supra note 6, § 801(c), 82 Stat. 197, 211-12; S. Rep. No. 1097, 90th Cong., 2d Sess. 70, 89, reprinted in 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2157, 2177. One scholar urges that the metaphor “war on crime” carries within it an inherent denigration of individual liberties. See Schwartz, supra note 6, at 43-45.*


*388 U.S. 41 (1967) (reversal of conviction for conspiracy to bribe a public official where conviction secured by invalid court-ordered eavesdrop). Berger delineated the constitutional prerequisites to the issuance of an eavesdropping warrant: (1) there must be probable cause to believe that a particular offense has been or is being committed; (2) the warrant must particularly describe the conversations to be intercepted; (3) eavesdropping must be limited in duration; (4) extensions may be granted only on a new showing of probable cause; (5) eavesdropping must terminate once the sought-for evidence has been obtained; (6) there must be a showing of*
INTERCEPTION OF COMMUNICATIONS

States10 as constitutional prerequisites to lawful court-authorized interception of private communications.11 Finally, it attempted to “define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.”12 Exigent circumstances to justify the lack of notice; and (7) there must be a return on the warrant. Id. at 54-60.

10 389 U.S. 347 (1967) (reversal of conviction for interstate transmission of wagering information where conviction secured with a wiretap that was a properly circumscribed surveillance, but was not duly authorized by a magistrate). Katz reaffirmed the principles of Berger, and also found that a neutral predetermination of the scope of the search by a magistrate is a “constitutional precondition” of electronic surveillance. Id. at 358-59. For a discussion of the effect of Berger and Katz on prior law, see Dash, Katz—Variations on a Theme by Berger, 17 Cath. U.L. Rev. 296 (1968). See also discussion at supra note 5.

11 See S. Rep. No. 1097, 90th Cong., 2d Sess. 74-75, reprinted in 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2161-62. Application of the Fourth Amendment to nontrespassory interception of communications carries with it, however, procedural and conceptual problems which do not arise in situations involving traditional search warrant litigation. First, the nature and scope of a search authorized by a traditional search warrant is substantially different than that authorized by an interception order. A traditional search warrant application must establish probable cause to believe that particularly described items will be found in a specified premises; an interception application, by contrast, must establish probable cause to believe that particularly described communications, which have not yet taken place, will be seized over a specified telephone or in a specified location. The traditional warrant authorizes a single, overt entry and search of the premises, and no second entry or search is permitted unless a new warrant, supported by a new showing of probable cause, is obtained; an interception order may authorize a series of surreptitious intrusions for several days or weeks on a single showing of proximate cause.

In addition to defining the nature and scope of the search, a second problem arises in defining the scope of authorized police conduct, and the remedy to be applied in the event of unauthorized conduct. When police execute a traditional search warrant, they usually know when they see an object whether it falls within the gambit of items subject to seizure. If the police seize more than a search warrant authorizes them to, the non-authorized items are inadmissible at trial and must be returned to the owner. Agents executing a wiretap or eavesdrop, by contrast, often cannot know whether a conversation constitutes the sought-for evidence until it has been heard in its entirety. Since restoration of conversational privacy is not possible, what remedy, if any, may be imposed to deter excessive overhearing?

The requirements for a Title III interception order are outlined in some detail in Part II of this Article, but in essence, such an order is a specialized form of search warrant. As such, it must comply with the warrant clause of the Fourth Amendment, which directs that "no warrants shall issue, but upon probable cause, supported by Oath or affirmation, particularly describing the place to be searched, and the person or thing to be seized." Accordingly, one of the preconditions to an interception order included in Title III is that investigators submit an application to a judge establishing probable cause to believe that evidence of specified criminal conduct could be obtained by monitoring conversations on the particular telephone to be tapped or in the particular location to be bugged.

The preparation of an application for an interception order is a time-consuming process, and properly so, since the decision to employ so intrusive an investigative technique should not be too easily or too lightly made. Inevitably, however, occasions arise in which investigators have to act promptly, or risk losing the opportunity to act effectively. Anticipating such occasions, Congress included within Title III a provision which permits, in certain limited situations, the interception of communications before a judge issues, or receives an application for, a court order authorizing such interceptions. This "emergency surveillance" provision was intended as a statutory analogy to the "exigent circumstances" doctrine, which holds that where the need for prompt action is particularly compelling, law enforcement officials may conduct a warrantless search, seizure or arrest in situations normally requiring a warrant.

Eighteen years later, Congress added a new provision to Title III which empowers federal officials, in certain circumstances, to obtain a court order permitting them to tap or bug the conversations of a suspect named in the order regardless of what telephone or location the suspect might choose to use on a particular day. The addition
of this "roving intercept" provision was a major development in Title III because it waived the otherwise rigid requirement that an intercept order must "particularly describe" the phone to be tapped or location to be bugged.

One might expect that federal investigators would frequently invoke the broad authority that Congress seems to have given them through the emergency surveillance and roving intercept provisions, but they have not. As of the summer of 1987, the Justice Department had not once utilized the roving intercept provision that was added to Title III in 1986,\(^{18}\) and had employed the Title III emergency surveillance provision only a handful of times in twenty years.\(^{19}\) The Department has apparently used the emergency surveillance provision only in life-threatening situations, and has been reluctant to apply it in a more straight-forward evidence gathering context.\(^{20}\)

To some extent, this reluctance is understandable: the procedures mandated in the emergency surveillance provision are cumbersome,\(^ {21}\) its vagueness raises questions of constitutional validity, and the vagueness of the constitutional "exigent circumstances" doctrine on which it is based creates even more uncertainty.\(^ {22}\) On the other hand, some may criticize the Justice Department's caution as excessive. It is probably impossible to determine how often an unwillingness to invoke the provision has hampered the effective use of wiretapping and eavesdropping. The need to invoke the emergency surveillance and roving intercept provisions is likely to increase in the future, however,
as advances in communications technology provide criminals with
greater opportunities for evasive tactics.\textsuperscript{23}

This Article will examine these provisions in their constitutional
and statutory contexts. Part I briefly reviews basic Fourth Amend-
ment case law regulating searches and seizures, summarizes the exi-
gent circumstances doctrine, and discusses the applicability of that
document to electronic surveillance of communications. Part II outlines
Title III's requirements for a "standard" (non-emergency, non-roving)
interception order, including what the application and order must
contain, and how such an order must be executed. Part III studies
the emergency surveillance provision of Title III and reviews Justice
Department policies and practices in implementing that provision.
Part IV analyzes the new roving intercept provision, discusses its
constitutionality, and looks at some practical problems that may arise
when obtaining and using an intercept order authorized under it.
Part V briefly examines how three other Western democracies, Can-
ada, Israel and West Germany, regulate emergency surveillance, and
compares their rules to our own. Part VI offers an evaluation of the
current system of regulation, and some proposed reforms.

I. THE FOURTH AMENDMENT AND WARRANTLESS INTERCEPTION OF
COMMUNICATIONS

A. The Warrant Requirement

\textsuperscript{23} For example, several recent court opinions have noted that narcotics viol-
ators are using telephone "beepers" or "pagers"; doing so permits them to stay
in telephone contact with coconspirators while minimizing the risk of wiretapping.
See, e.g., United States v. Cox, 752 F.2d 741, 744 (1st Cir. 1985) (DEA agent
called the beeper number and the suspect returned the call); United States v.
Marin-Buitrago, 734 F.2d 889, 891 (2d Cir. 1985) (one of the grounds given by
a DEA agent to substantiate probable cause for a warrant was the use of a beeper
in premises where tenants did not have a telephone); United States v. Ginsberg,
758 F.2d 823, 827 (2d Cir. 1985) (officers found on suspect a beeper and access
number to another suspect's beeper); United States v. Williams, 753 F.2d 329,
334 (4th Cir. 1985) (beeper found in suspect's possession at arrest); United States
v. Antone, 753 F.2d 1301, 1305 (5th Cir. 1985) (evidence of beeper use helped
sustain guilty plea). Similarly, numerous cases have arisen recently in which the
suspects have used telex or other forms of "electronic mail" in their criminal
schemes. See, e.g., Howitt, Court Pris into E-Mail, Infoworld, July 15, 1985, at
26; Iranian Accused of Conspiring to Export Military Equipment, Baltimore Sun,
June 28, 1985, at 1C, col. 1; Raytown Couple Indicted, Kansas City Times, Feb.
The Fourth Amendment prohibits unreasonable searches and seizures, and imposes strict requirements on the warrants that may be issued for reasonable searches and seizures. Under the "Fourth Amendment exclusionary rule," if evidence is obtained in a manner which violates a defendant's Fourth Amendment rights, the prosecutor is not permitted to use that evidence at trial to establish that defendant's guilt. Searches conducted without a warrant have been found "presumptively unreasonable" by the Supreme Court, and the fruits of those searches are generally subjected to the exclusionary rule.

---

24 The fourth amendment provides, in full:

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.

U.S. Const. amend. IV.

25 Weeks v. United States, 232 U.S. 383, 398 (1914) (first case in which the Court applied the rule in a federal prosecution). See also Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that the exclusionary rule is binding on state courts through the due process clause of the fourteenth amendment). The exclusionary rule is intended to deter law enforcement officials from conducting unlawful searches and seizures by depriving them of the incentive to do so. Nix v. Williams, 467 U.S. 431, 441-47 (1984); United States v. Ceccolini, 435 U.S. 268, 275-76 (1978); Stone v. Powell, 428 U.S. 465, 486 (1976); United States v. Janis, 428 U.S. 433, 458 n.35 (1976); United States v. Calandra, 414 U.S. 338, 348 (1974); Mapp v. Ohio, 367 U.S. at 657-68. In Mapp, the Court emphasized other purposes for the rule as well, including "the imperative of judicial integrity," id. at 659 (quoting Elkins v. United States, 364 U.S. 206, 222 (1960)), but more recently the Court has stressed the deterrent rationale as the primary justification for the rule. See cases cited above.

26 United States v. Karo, 468 U.S. 705, 717 (1984). See also Katz v. United States, 389 U.S. 347, 357 (1967) (finding that warrantless searches "are per se unreasonable under the Fourth Amendment ... "). The Supreme Court has stated that the purpose of the warrant requirement is to allow a neutral judicial officer to assess whether the police have probable cause to make an arrest or conduct a search.... [T]he placement of this checkpoint between the Government and the citizen implicitly acknowledges that an 'officer engaged in the often competitive enterprise of ferreting out crime' may lack sufficient objectivity to weigh correctly the strength of the evidence supporting the contemplated action against the individual's interests in protecting his own liberty and the privacy of his home. Steagald v. United States, 451 U.S. 204, 212 (1981) (citations omitted) (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)).
Nonetheless, the Supreme Court has recognized several exceptions to the warrant requirement. For example, a warrant usually is not required to authorize a search of an automobile, or containers found therein, so long as probable cause exists to believe that the search will reveal evidence of criminal activity.\textsuperscript{27} Also, if a person is lawfully arrested, the police may conduct a search incident to that arrest. Such a search can include the arrestee himself,\textsuperscript{28} personal property on or in the possession of the arrestee,\textsuperscript{29} and the area "within [the] immediate control" of the arrestee at the time of the arrest.\textsuperscript{30} A search conducted pursuant to consent is also excepted from the warrant requirement.\textsuperscript{31} Finally, the Court has recognized an exception that is very important in the warrantless interception of communications, the "exigent circumstances" exception, which is discussed below.

\footnotesize
\textsuperscript{30} New York v. Belton, 453 U.S. 454, 457-62 (1981) (where arrest occurs while or immediately after an arrestee is inside an automobile, a police officer may, as a contemporaneous incident of that arrest, search the passenger compartment of the automobile, and may examine the contents of any containers found within the passenger compartment); Chimel v. California, 395 U.S. 752, 763 (1969) (where arrest occurs within a home or other premises, search incident must be limited to the "area from which [the arrestee] might gain possession of a weapon or destructible evidence"). Even in the absence of probable cause either to arrest or to search, in certain circumstances the police are permitted to conduct a limited search of a suspect or his automobile. The Supreme Court has held on several occasions that an officer may stop (seize) and frisk (search) a suspect whom the officer reasonably believes is armed and dangerous, provided that the search is carefully limited to a frisk for weapons. Pennsylvania v. Mimms, 434 U.S. 106, 112 (1977); Adams v. Williams, 407 U.S. 143, 146 (1972); Terry v. Ohio, 392 U.S. 1, 24-27 (1968). See also Michigan v. Long, 463 U.S. 1032, 1049 (1983) (permitting a limited search of passenger compartment for weapons in stop-and-frisk situation); Michigan v. Thomas, 458 U.S. 259, 261 (1982) (upholding "inventory" search of impounded car in the absence of a warrant, exigent circumstances and, apparently, probable cause).
\textsuperscript{31} Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (stolen checks found in trunk of car found admissible where owner voluntarily told police to "go ahead" if they wanted to search).
B. The "Exigent Circumstances" Doctrine

The Supreme Court has long recognized that in some circumstances "the exigencies of the situation" make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.\(^3\) Such situations are divisible into three general categories: life-threatening exigencies, hot pursuit, and preservation of evidence from destruction.

1. Life-Threatening Exigencies. The most obvious "exigent circumstance" exists where police have reason to believe that someone inside the premises in question is in immediate danger of death or permanent injury. "[T]he Fourth Amendment does not bar police officers from making warrantless entries and searches when they reasonably believe that a person within is in need of immediate aid,"\(^3\) and the case law indicates that this rule applies whether the danger is criminal or noncriminal in origin.\(^3\) Because such entries are lawful, evidence discovered in plain view as a result of such entries may lawfully be seized and is admissible at trial.\(^3\)

2. Hot Pursuit. A second exigent circumstance arises when police are in "hot pursuit" of a suspect who flees into a building and hides there. Assuming probable cause exists to arrest the suspect, the police

\(^3\) Mincey v. Arizona, 437 U.S. 385, 394 (1978) (invalidating an Arizona "murder scene exception" to the warrant requirement, and holding that a possible homicide does not inevitably create an emergency situation); Chimel v. California, 395 U.S. 752, 763 (1969) (recognizing exception to search for weapon or destructible evidence, but finding a search beyond this unreasonable); Warden v. Hayden, 387 U.S. 294, 298-300 (1967) (exception recognized when officers in "hot pursuit"); Schmerber v. California, 384 U.S. 757, 770-71 (1966) (recognizing exception to prevent destruction of evidence); Johnson v. United States, 333 U.S. 10, 14-15 (1948) (recognizing exception, but finding only inconvenience and slight delay would have resulted from obtaining warrant); McDonald v. United States, 335 U.S. 451, 456 (1948) (recognizing exception, but finding insufficient exigency).

\(^3\) Mincey, 437 U.S. at 392 (citing numerous state and lower federal court decisions). Cf. New York v. Quarles, 467 U.S. 649, 655-56 (1984) (recognizing an analogous "public safety" exception to the rule, enunciated in Miranda v. Arizona, 384 U.S. 436, 436 (1966), that various warnings must precede custodial interrogation before statements obtained as a result of such interrogation are admissible at trial).


may enter the premises without a warrant. Once inside, they may search for the suspect, for other individuals who might endanger the police or who might themselves be endangered, and for weapons. Evidence discovered during such a search may lawfully be seized and is admissible at trial.

3. Preserving Evidence from Destruction. The Supreme Court has frequently acknowledged that where the delay necessary to obtain a warrant threatens the destruction of evidence, a warrantless seizure, entry or search is not a violation of the Fourth Amendment. The Court's decisions provide only general guidance, however, as to when warrantless action to prevent the destruction of evidence is lawful. There is great uncertainty regarding the degree of emergency or exigency necessary to excuse the absence of a warrant.

To date, there has been only one case, *Schmerber v. California*, in which a majority of the Supreme Court has upheld a warrantless search on preservation-of-evidence grounds. Since the "search" in

---

38 Id. at 300-10.
40 384 U.S. 757 (1966). The defendant, Schmerber, had been involved in a traffic collision under circumstances establishing probable cause that he was driving while intoxicated. After taking Schmerber to a hospital, the arresting officer directed a doctor to remove a blood sample which confirmed that Schmerber was intoxicated. Under the circumstances, the Court concluded "there was no time to seek out a magistrate and secure a warrant." *Id.* at 771. The Court found that it was reasonable for the officer to have the doctor take a blood sample since Schmerber had refused to submit to a breathalyzer test, and that the procedure was conducted in a reasonable manner. *Id.*.
41 A case which is relevant but provides no binding precedent is *Ker v. California*, 374 U.S. 23 (1963), in which police, acting without a search warrant, obtained a key to the home of a drug suspect, entered without first knocking and giving notice, and seized additional contraband. The state courts had upheld the action, reasoning that entry without notice was justified under the circumstances because to give notice would have afforded the suspect time to destroy the drugs that police had reason to believe were inside. Four Justices of the Supreme Court agreed with the state court reasoning, and four Justices dissented. Justice Harlan, the remaining voice, decided to uphold the state court decision, but on the ground
that case was the taking of a blood sample to determine the presence of alcohol, it differs from most evidence-preservation warrantless searches in at least two significant respects: the blood-alcohol evidence was extremely evanescent, and the "place to be searched" was the body of a defendant already in custody. Thus, Schmerber offers little direct guidance in determining the degree of exigency required to justify the nonwarrant entry into someone's home, office or other location to search for less inherently evanescent evidence.

Although the Court has rejected several governmental claims of adequate exigency, these decisions are not very enlightening as to the degree of exigency that would have sufficed. In Johnson v. United States, the Court found insufficient exigency to justify a warrantless search of a hotel room, from which the aroma of burning opium was emanating, because "[n]o evidence or contraband was threatened with removal or destruction, except perhaps the fumes which we suppose in time would disappear." In Vale v. Louisiana, the Court arrived at the same result, explaining that "[t]he goods ultimately seized were not in the process of destruction. Nor were they about to be removed from the jurisdiction."

Given the rate at which the body eliminates alcohol from the system, it was a virtual certainty in Schmerber that the evidence would have been lost if the officer had waited until he obtained a warrant. Schmerber, 384 U.S. at 770. The Court stated that "absent an emergency, no less [than a search warrant] could be required where intrusions into the human body are concerned," id., but does not elaborate on whether more should be required, or the effect of custody.

333 U.S. 10 (1948).

Id. at 15. This was a curious comment, since, at the very least, the opium being smoked was in the process of being destroyed when the officers knocked on the door.


Id. at 35 (citations omitted). The dissenting opinion notes that none of the decisions cited by the majority support the proposition that contraband must be "in the process of destruction" to invoke the exigent circumstances doctrine, but only that it must be "threatened with removal or destruction." Id. at 39 (Black, J., joined by Burger, C.J., dissenting). Police officers arrested Vale just outside his home under circumstances establishing probable cause that he had narcotics inside the home. Concerned that someone inside might have seen the arrest and would destroy the drugs before they could obtain a warrant, the officers made a
Arizona, the Court condemned a warrantless search of a homicide scene because "[t]here was no indication that evidence would be lost, destroyed, or removed during the time required to obtain a warrant."

Three decisions handed down in 1984 reinforced the existence of the exception, but did little to dissipate the uncertainty of its scope. Suppressing evidence of arson found after a residential fire in Michigan v. Clifford, the Court nevertheless commented that warrantless entry and search "may [under different circumstances] be necessary to preserve evidence from intentional or accidental destruction." In United States v. Karo, the Court held that monitoring an electronic tracking device inside someone's home normally must be authorized by a warrant but that "if truly exigent

cursory inspection of the home to determine if anyone was present. No one was inside, but the mother and brother of the arrested party returned home within minutes. The officers then proceeded to search the house, and seized a quantity of narcotics. Id. at 32-33.

The Supreme Court concluded that the search was illegal. "We decline to hold that an arrest on the street can provide its own 'exigent circumstance' so as to justify a warrantless search of the arrestee's house." Id. at 35. It is not altogether clear, however, whether the Court was condemning the initial entry into the house to determine whether it was occupied, or only the more detailed search which resulted in the discovery of the narcotics. See id. at 34. Further, the Court apparently assumed that the police had had probable cause for a warrant to search the house even before they set up their surveillance of it. Id. at 35.

49 Id. at 394. Officers went to Mincey's apartment to arrest him for a previous sale of narcotics. A shootout ensued, and a police officer was killed. Over the next four days, homicide detectives returned to the apartment on several occasions to search every corner of it. The Court rejected the state's contention that an implicit "homicide scene" exception existed to the Fourth Amendment warrant requirement. Id. at 395. "Except for the fact that the offense under investigation was a homicide," the Court observed, "there were no exigent circumstances in this case, . . . ." Id. at 394. The Court took note of the fact that a police guard at the apartment precluded the removal or destruction of evidence, and that "there was no suggestion that a search warrant could not easily and conveniently have been obtained." Id. at 394.


51 Id. at 293 n.4 (quoting Michigan v. Tyler, 436 U.S. 499, 510 (1978)). The Court held that "where a homeowner has made a reasonable effort to secure his fire-damaged home after the blaze has been extinguished and the fire and police units have left the scene, . . . a subsequent post-fire search must be conducted pursuant to a warrant, consent, or the identification of some new exigency." Id. at 297.

circumstances exist no warrant is required under general Fourth Amendment principles.\(^5\) Finally, in *Welsh v. Wisconsin*,\(^6\) the Court concluded that "mere similarity to other cases involving the imminent destruction of evidence is not sufficient" when the offense being investigated is so minor as to be classified as noncriminal.\(^5\)

Thus, while the Court has firmly established the exception to the warrant requirement for evidence preservation in exigent circumstances, it has done little to define the scope of that exception. It is unclear whether the prosecution must prove that the evidence was "threatened with removal or destruction,"\(^5\) that it was "in

\(^5\) *Id.* at 718. In *Karo*, drug enforcement agents installed a "beeper" in a drum of chemicals in the hope of locating a clandestine laboratory. The Court held that no warrant was needed to justify the installation of the beeper, *id.* at 713, but that, barring exigent circumstances, a warrant was required before law enforcement officials could monitor the beeper once its host object has been taken into a private residence. *Karo* is discussed at *infra* notes 84, 85, 258, 288-292 and accompanying text. For a detailed analysis of the case, see Fishman, *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered*, 34 CATH. U.L. REV. 277-395 (1985).


\(^5\) *Id.* at 753-54. Arriving at the scene shortly after the defendant had driven his car off the road into an open field, police officers were told by a witness that the driver appeared to have been "very inebriated or very sick," *id.* at 742, but had walked away. The police checked the car's registration, obtained the driver's home address, entered the home when the driver's stepdaughter answered the door, and found him lying naked in his bedroom. *Id.* at 742-43. They arrested him and took him to the police station where he refused to take a breath-analysis test. According to state law, the arrestee's operating privileges would be revoked for 60 days, and his refusal to take the test admissible against him in a criminal proceeding for driving while intoxicated, unless he could show that the refusal was reasonable. *Id.* at 746-47.

The defendant maintained that his refusal was reasonable because he was unlawfully placed under arrest subsequent to an illegal search. The trial court disagreed, but the appellate court reversed, finding a Fourth Amendment violation. *Id.* The state supreme court reversed, finding exigent circumstances in the need for hot pursuit of a suspect, the need to prevent physical harm to the offender and the public, and the need to prevent destruction of evidence (the blood-alcohol level). *Id.* at 748.

The U.S. Supreme Court found no hot pursuit or threat of harm. It assumed that there was an exigent circumstance due to the threat of destruction of evidence, *id.* at 754, but also found that "an important factor to be considered when determining whether any exigency exists is the gravity of the underlying offense for which the arrest is being made." *Id.* at 753. Noting that Wisconsin classified an initial offense for driving while intoxicated as noncriminal, the Court concluded that the warrantless entry into Welsh's home was indeed illegal.

the process of destruction" or "about to be moved," or only
that there is an "indication that evidence would be lost, destroyed
or removed," even assuming that the offense under investigation
is serious enough.

Nonetheless, we may make some general observations regarding
the conditions under which the exigent circumstances doctrine may
be invoked. The decisions cited above, "general Fourth Amendment
principles, and decisions of lower courts" suggest the following
requirements:

1. Exigencies aside, there must be grounds for a warrant.
   This means that there must be probable cause to believe
   that particular evidence will be found in a particular
   premises.

2. The circumstances must be sufficiently exigent. The
   factors to be considered in assessing exigency include:
   a. the gravity of the underlying offense;
   b. whether the evidence is readily susceptible to re-
      moval or destruction;

---

   United States Dist. Court, 407 U.S. 297, 318 (1972) (holding that a warrant was
   required to wiretap or eavesdrop upon a domestic group or organization for
   national security purposes, but also recognizing that the exceptions to the warrant
   requirement "serve the legitimate needs of law enforcement officers to protect
   their own well-being and preserve evidence from destruction"); United States v.
   Jeffers, 342 U.S. 48, 52 (1951) (rejecting a warrantless search, in part because
   there "was no question of . . . imminent destruction, removal or concealment of
   the property intended to be seized"); McDonald v. United States, 335 U.S. 451,
   455 (1948) (reaching the same result because, among other reasons, there was no
   "property in the process of destruction" or "likely to be destroyed").

60 "If truly exigent circumstances exist no warrant is required under general
61 Perhaps the most detailed discussion of the issue appears in United States
62 The analysis that follows is based in significant part on W. LaFAVE, supra
   note 34, § 6.5, at 439-50.
   U.S. 10, 13 (1948).
65 Ker v. California, 374 U.S. 23, 40 (1963) (plurality opinion, discussed supra
   note 41); United States v. Rubin, 474 F.2d 262, 268-270 (3d Cir. 1973).
c. The amount of time necessary to obtain a warrant; 66
d. whether the officers have a valid basis to believe that the evidence is likely to be removed or destroyed while a warrant is being obtained; 67
e. whether the police failed to take advantage of an earlier opportunity to obtain a warrant, or earlier sought a warrant and were turned down for lack of probable cause; 68
f. whether the exigency was unnecessarily provoked by the police themselves; 69
and
g. whether the police attempted to obtain a warrant at the earliest opportunity. 70

3. The measures taken to meet the exigency must be inherently reasonable under the circumstances. 71

4. The search or seizure in question must be conducted in a reasonable manner. 72

C. Applicability of the "Exigent Circumstances" Doctrine to Electronic Surveillance

For many years, the Fourth Amendment was found inapplicable to electronic surveillance unless government officials had physically trespassed on the defendant's premises. 73 In Katz v. United States, 74

---

66 Rubin, 474 F.2d at 269-70.
67 Whether to require "probable cause" or a lesser standard, such as "reasonable suspicion," remains the most difficult question. See, e.g., United States v. Karo, 468 U.S. 705, 718 n.5 (1984) (expressly reserving the question of whether reasonable suspicion may be sufficient to justify a warrant for monitoring a beeper). With regard to interception of communications, however, there will almost always be probable cause to believe that the evidence sought will be unavailable by the time a warrant is obtained.
69 W. LaFave, supra note 34, § 6.5, at 442.
70 Id. at 441.
72 Id. at 771.
73 See supra note 5.
however, the Supreme Court held that the use of an electronic
device to overhear a private conversation constituted a search
regardless of whether the authorities had trespassed onto the target's
property or premises to install the device.\textsuperscript{75} Thus, the interception
of private communications is now subject to the requirements and
restrictions imposed by the Fourth Amendment.\textsuperscript{76}

Some dicta in the \textit{Katz} case suggested that the exceptions to the
warrant requirement might never apply to electronic surveillance,\textsuperscript{77}
and some commentators have expressed doubts about the constitutionality of intercepting communications without a warrant under
any circumstances.\textsuperscript{78} It is clear, however, that the difficulties the
Court spoke of were of a practical, rather than a constitutional,
nature.\textsuperscript{79} For example, in its discussion of the life-threatening cir-
cumstances exception, the Court did not find the exception inap-
licable per se; rather, it assumed that "there seems little likelihood
that electronic surveillance would be a realistic possibility in a sit-
uation so fraught with urgency."\textsuperscript{80} In addition, the Court did not
even address the most relevant exigent circumstances exception,
preservation of evidence.\textsuperscript{81} The \textit{Katz} dicta is, therefore, an insuffi-
cient basis for the argument that exigent warrantless surveillance

\textsuperscript{75} \textit{Id.} at 353 (expressly overruling earlier decisions supporting the "trespass
document"). In \textit{Katz}, law enforcement officials placed an eavesdropping device on
the outside of a public telephone booth, which enabled them to overhear Katz
relating gambling information into the telephone. \textit{Id.} at 348.

\textsuperscript{76} \textit{Id.} at 353-54. The \textit{Katz} Court found that the warrantless voice recordings
did not comply with "constitutional standards," \textit{id.} at 354, even though the agents
acted "with restraint," \textit{id} at 356, because the restraint was not imposed by a
judicial officer, \textit{id.}, and none of the recognized exceptions to the warrant require-
ment where shown, \textit{id.} at 357-58.

\textsuperscript{77} "It is difficult to imagine how any of those exceptions [to the warrant
requirement] could ever apply to the sort of search and seizure involved in this
case." \textit{Katz}, 389 U.S. at 357.

\textsuperscript{78} \textit{NWC Report, supra} note 6, at 15-16 (1976) (acknowledging such doubts
while not agreeing with them).

\textsuperscript{79} \textit{See Katz} v. United States, 389 U.S. 347, 357-58 (1967) (discussing the search
incident to arrest, hot pursuit, life-threatening and consent search exceptions to
the warrant requirement).

\textsuperscript{80} \textit{Id.} at 358 n.21. The Court was wrong in its prediction: the Justice De-
partment reports that it has used such surveillance successfully in several instances.
See \textit{infra} note 172.

\textsuperscript{81} The Court had recognized this exception at least 19 years earlier in \textit{Johnson
v. United States}, 333 U.S. 10, 15 (1948). \textit{See also supra} notes 39-59 and accom-
panying text (authority for the exception).
INTERCEPTION OF COMMUNICATIONS

is inherently unconstitutional. Further, it may reasonably be construed to mean that the Court will apply the exigent circumstances doctrine to electronic surveillance as a matter of law if an appropriate case comes before it.

In subsequent decisions, the Court has said nothing to suggest that exigent warrantless interceptions are inherently unconstitutional. Indeed, in United States v. Karo, a case involving electronic tracking devices, a form of surveillance concededly less intrusive than the interception of communications, the Court seemingly went out of its way to comment that "if truly exigent circumstances exist no warrant is required under general Fourth Amendment principles." It seems logical to conclude, therefore, that exigent warrantless electronic surveillance is constitutional so long as it complies with the same Fourth Amendment standards against which exigent warrantless physical searches are measured. Applying those standards in the context of life-threatening exigencies presents little difficulty.

Application of the exigent circumstances doctrine to electronic surveillance in the context of preserving evidence from destruction, on the other hand, presents at least two major problems. First, the standards governing exigent physical searches and seizures are as yet only vaguely developed. It is obviously problematic to apply "standards" to a new situation when the standards themselves are ill-defined. Second, an electronic "search" for and "seizure" of a private conversation bears so little resemblance to a physical search and seizure that analogies from the law governing the latter apply imperfectly and awkwardly to the former.

82 In United States v. United States Dist. Court, 407 U.S. 297, 308 (1972) the Court, while rejecting the Government's claim that it had implicit constitutional power to conduct warrantless electronic surveillance against a domestic group for national security purposes, observed that the established exceptions to the warrant requirement, "few in number and carefully delineated, . . . serve the legitimate needs of law enforcement officers to protect their own well-being and preserve evidence from destruction." The reference to the preservation of evidence was dictum, but is at least consistent with the constitutionality of warrantless surveillance.


84 Id. at 718. The Court's comment was completely gratuitous; the government had not raised an exigent circumstances argument in its briefs or during oral argument.

85 See supra notes 32-72 and accompanying text.

86 See supra note 11.
Let us assume, for example, that the Supreme Court holds that a warrantless physical search to preserve evidence from destruction is constitutionally permissible only when the crime under investigation is a felony\(^8\) and the evidence in question was "in the process of destruction."\(^8\) Such a standard would place a near-impossible burden on law enforcement officials in the physical search context. Arguably, however, it would do little to limit warrantless interception of communications. This is so because these interceptions are most frequently used to detect felonies\(^9\) and the evidence sought by such surveillance is inherently evanescent—it must be recorded immediately or lost for good. Considerations of public policy, and perhaps the Fourth Amendment, demand a distinct standard of exigency in the context of electronic surveillance that will take these factors into account.

A variety of factors seem relevant in defining a practicable standard. The nature of the crime under investigation should be considered.\(^9\) The importance, in the context of the investigation, of the communications that may be reasonably expected to occur before an application for a court order may be submitted and acted upon is of crucial relevance, as is the likelihood that substantially similar conversations will occur after a court order is obtained.\(^9\)

\(^8\) Such a holding might result from an extension of the ideas in Welsh v. Wisconsin, 466 U.S. 740, 753-54 (1984). See supra notes 54-55 and accompanying text.

\(^8\) This requirement might be derived from a narrow reading of Vale v. Louisiana, 399 U.S. 30, 35 (1970). See supra notes 46-47 and accompanying text.


\(^9\) In an investigation of a continuing crime, such as narcotics trafficking, gambling, or fencing, it is often reasonable to assume that even if the details of a particular transaction are missed while a court order is being sought, substantially similar transactions will continue to occur after an order is issued. In such situations, no exigency exists that would justify warrantless surveillance. This type of investigation comprises the overwhelming majority of applications made pursuant to Title III and corresponding state statutes.

In 1984, for example, federal judges issued 289 wiretapping or eavesdropping orders, and state judges issued 512. Of this total of 801 interception orders, 483 (60.3% of the total) were issued to investigate narcotics, in 186 (23.2%), the most serious offense was gambling, in 53 (6.6%), the main offense was racketeering.

Report on Applications for Orders Authorizing or Approving the Intercep-
The delineation of such standards is appropriately a legislative rather than a judicial function.

Parts III and IV of this Article examine how Congress has attempted to regulate warrantless surveillance through the emergency surveillance and roving interception provisions of Title III. To put these provisions in context, however, it is first necessary to review how Title III regulates court-ordered interception of communications.

II. TITLE III: PREREQUISITES TO COURT-ORDERED SURVEILLANCE

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 empowers law enforcement officials to seek, and judges to issue, court orders authorizing the interception of "wire communications," "oral communications," and, since 1986, "electronic communications." On the other hand, if investigators have been tracking the progress of a particular major transaction and learn that the deal will be finalized in a phone call or meeting before a court order can be obtained, a true exigency exists which should justify warrantless surveillance for a limited period of time while an interception application is being prepared. Justice Department officials, however, doubt the need for nonwarrant emergency even in these circumstances. See infra note 208 and accompanying text.

92 Title III, supra note 6.

93 Title III defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (1982). For a detailed discussion of the definition, see C. FISCHER, WIRETAPPING AND EAVESDROPPING § 7.2 (1987). Certain categories of interceptions, such as particular activities of switchboard operators, employees of communications common carriers, and the Federal Communication Commission ["F.C.C."] are exempted from the warrant requirement of Title III. 18 U.S.C. §§ 2511(2)(a), (b) (1982). Persons "acting under color of law" are authorized to intercept wire, oral and electronic communications without a warrant so long as one participant to the conversation consents in advance. Id. § 2511(2)(c). Private citizens are also permitted to do this, assuming a participant consents in advance and the conversation is not being intercepted for an unlawful or tortious purpose. Id. § 2511(2)(d). For a detailed discussion of consensual interceptions, see Fishman, The Interception of Communications Without a Court Order: Title III, Consent, and the Expectation of Privacy, 51 St. John's L. Rev. 41-98 (1977); C. FISCHER, supra, §§ 8-19.

94 Title III defines "wire communication," in pertinent part, as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. . . ." 18 U.S.C. § 2510(1) (Supp.
It is a detailed legislative scheme which specifies who may authorize an investigator to apply for a court order, the information an application must contain and the findings a judge must make before issuing the order, how the order is to be executed, how recordings of intercepted conversations are to be secured, who must eventually receive notice that a phone was tapped or a location was bugged, and a host of other items. The statute describes when information obtained from intercepted communications may be disclosed, identifies who may seek to suppress evi-

IV 1986). "Aural transfer" is defined as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18) (Supp. IV 1986). Although these definitions were amended in the ECPA, supra note 17, the 1986 amendments have no material effect on this discussion. For a detailed discussion of these definitions, see C. Fishman, supra note 93, § 7.5 (wire communication); id. § 7.17 (aural transfer).

Title III defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." 18 U.S.C. § 2510(2) (Supp. IV 1986). Although this definition was added to Title III by the ECPA, supra note 17, the 1986 amendment has no material effect on this discussion. For a detailed discussion of these definitions, see C. Fishman, supra note 93, § 7.4.

"Electronic communication" is defined in 18 U.S.C. § 2510(12). In essence, it includes many forms of radio communications, electronic mail and computer-to-computer transmissions. For a detailed discussion, see C. Fishman, supra note 93, § 7.22. This definition was added to Title III by the ECPA, supra note 17, a major feature of which is the statutory protection of the privacy of such communications. The law governing interception of electronic communications is similar to that regulating interception of wire and oral communications, but in several significant respects it is easier to obtain a court order authorizing interception of the former than it is authorizing interception of the latter two.

See infra note 112 and accompanying text.

See infra notes 108-23 and accompanying text.

See infra notes 150-58 and accompanying text.

18 U.S.C. § 2518(8)(a) (Supp. IV 1986) requires recordings to be made available to the judge who issued the order, and "sealed under his directions." For a detailed discussion of the sealing requirement, see C. Fishman, supra note 93, §§ 191-202.


18 U.S.C. § 2517 (Supp. IV 1986). In essence, disclosure is permitted only when there is a valid law enforcement purpose for such disclosure. See C. Fishman, supra note 93, §§ 148-148.3, 163-165.
dence and on what grounds,\textsuperscript{103} and sets forth an exclusionary rule.\textsuperscript{104} It also creates a civil cause of action for those whose communications are unlawfully intercepted.\textsuperscript{105}

In drafting the legislation in 1968, Congress sought to incorporate the constitutional prerequisites that the Supreme Court had recently enunciated in \textit{Katz v. United States}\textsuperscript{106} and, even more explicitly, in \textit{Berger v. New York}.\textsuperscript{107} The statute does more, however, than merely parallel the Fourth Amendment and Supreme Court decisions. Congress included within the statute several procedural and substantive safeguards that are not constitutionally mandated, many of which are not applicable to conventional search warrants. The discussion below reviews the required contents of a non-emergency Title III application and order, examines the statutory provisions regulating how such orders are to be executed, and reviews Supreme Court decisions construing these provisions.

\textbf{A. Application and Order}

\textit{1. In general.} Because an interception order is in essence a special kind of search warrant, it must comply with the Fourth Amendment directive that "no Warrants shall issue, but upon probable cause, ... particularly describing the place to be searched, and the persons or things to be seized."\textsuperscript{108} Title III therefore requires an application for an interception order to establish probable cause to believe "that an individual is committing, has committed, or is about to commit a particular offense,"\textsuperscript{109} and probable cause to believe that "particular communications concerning that offense will

\begin{itemize}
\item \textsuperscript{103} 18 U.S.C. § 2518(10)(a) (Supp. IV 1986) provides that any "aggrieved person" may move to suppress wire, oral, or electronic communications on the ground that the communication was "unlawfully intercepted," or was intercepted pursuant to a facially invalid order, or was intercepted in violation of the terms of the interception order. For a discussion of Supreme Court interpretation of the phrase "unlawfully intercepted," see infra notes 140-49 and accompanying text. Suppression of intercepted electronic communications may be sought only for constitutional, not statutory, violations. 18 U.S.C. § 2518(10)(c) (Supp. IV 1986).
\item \textsuperscript{104} 18 U.S.C. § 2515 (Supp. IV 1986) prohibits the receipt in evidence of intercepted communications or derivative evidence if the disclosure of that information would violate Title III.
\item \textsuperscript{105} 18 U.S.C. § 2520 (Supp. IV 1986). A good-faith reliance on a court order is a defense to such an action. Id. § 2520(d).
\item \textsuperscript{106} 389 U.S. 347 (1967). \textit{Katz} is briefly summarized in supra notes 5, 74-75.
\item \textsuperscript{107} 388 U.S. 41 (1967). \textit{Berger} is summarized in supra note 9.
\item \textsuperscript{108} U.S. \textbf{C}ont. amend. IV (quoted in full at supra note 24).
\item \textsuperscript{109} 18 U.S.C. § 2518(3)(a) (1982).
\end{itemize}
be obtained” by intercepting communications over the targeted facilities or in the targeted premises.\(^\text{110}\) Each application and order must contain a “particular description of the type of communication[s] sought to be intercepted.”\(^\text{111}\)

In addition, Congress has interposed several extra-constitutional requirements. A federal investigator or prosecutor may apply to a judge for an interception order only if he or she has first been authorized to do so by “the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General.”\(^\text{112}\) Title III also restricts the crimes which may be investigated by means of an interception order.\(^\text{113}\) Further, an application must inform the judge of all known prior applications “involving any of the same persons, facilities or places,” and whether any such prior application was granted or denied.\(^\text{114}\) Moreover, the application must satisfy the judge that “normal investigative procedures have been tried and have failed or reasonably

\(\text{\textsuperscript{110}}\) Id. §§ 2518(3)(b), (d) (1982 & Supp. IV 1986). Concerning the roving interception provision, in which the targeted facilities or premises are more uncertain, see infra notes 210-83 and accompanying text.


\(\text{\textsuperscript{112}}\) 18 U.S.C. § 2516(1) (Supp. IV 1986). The Senate Judiciary Committee Report on Title III explains:

This provision centralizes in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques. Centralization will avoid the possibility that divergent practices might develop. Should abuses occur, the lines of responsibility lead to an identifiable person. This provision in itself should go a long way toward guaranteeing that no abuses will happen.


\(\text{\textsuperscript{113}}\) 18 U.S.C. § 2516(1) (Supp. IV 1986). Compare FED. R. CRIM. P. 41 (permitting an agent to seek, and a judge or magistrate to issue, a search warrant to search for evidence relating to any criminal offense).

\(\text{\textsuperscript{114}}\) 18 U.S.C. § 2518(1)(e) (Supp. IV 1986). The provision acts as a check against “judge shopping” in the case of a previously rejected application. It also alerts the judge to inquire about the results of a prior tap or bug if agents seek a new order to investigate someone who had previously been targeted.
appear to be unlikely to succeed if tried or to be too dangerous.115

Unlike a conventional search warrant, which may be issued by a federal magistrate, only a federal district or circuit court judge may issue an interception order.116 The judge is empowered to reject the application even if it complies fully with statutory requirements.117 The judge also is authorized to require the investigators to submit to the court periodic reports disclosing what progress has been made toward accomplishing the goals of the investigation, thereby allowing the judge to assess the necessity for continued surveillance.118

The application and order must specify the period of time during which interceptions are to be conducted,119 and the order must also specify whether it authorizes the interception of more than one incriminating conversation.120 Interceptions must cease when the authorized objective has been attained.121 Special provisions govern extension of the initial order.122

Two of the requirements discussed above are of particular interest here, because of the way Congress treated them in the “roving intercept” provision.123 These are the “particular description” provisions, and the identification requirement.

2. Particularity. Title III requires an application for an interception order to include:

- a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to

115 18 U.S.C. § 2518(3)(c) (1982). There is no corresponding precondition for a search warrant. Indeed, in the Title III context, a search warrant is a normal, less intrusive procedure, the probable non-sufficiency of which must be explained before an intercept order may issue.
123 See infra notes 219-48 and accompanying text.
the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection 11, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; . . . .124

Congress included these provisions under the assumption that "[e]ach of these requirements reflects the constitutional demand of particularization."125

Similarly, the interception order itself must specify, among other information,

(a) the identity of the person, if known, whose communications are to be intercepted;
(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;
(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; . . . .126

Thus, the Senate Judiciary Committee Report on Title III observed, "the order will link up specific person, specific offense, and specific place. Together [these requirements, coupled with the probable cause requirement] are intended to meet the test of the Constitution that electronic surveillance techniques be used only under the most

124 18 U.S.C. § 2518(1)(b) (Supp. IV 1986) (emphasis added). The italicized phrase was added by the ECPA, supra note 17, to reflect the addition of section 2518(11), the roving intercept provision. Similarly, section 2518(3)(d) provides that a judge may issue an order only if, "except as provided in subsection 11, there is probable cause for belief that the facilities from which, or the place where, the . . . communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, . . . ." 18 U.S.C. § 2518(3)(d) (Supp. IV 1986) (emphasis added).


precise and discriminate circumstances, which fully comply with the requirement of particularity."

The statute, and the passages from the Senate Judiciary Committee Report quoted above, speak in terms of "specific person, specific offense, and specific place," but the degree of specificity required was left for the courts to determine. The statutory language left uncertainties as to what the application and order must say and the degree of latitude to be afforded investigators in executing the order.

a. "Specific offense." Most interception orders have been granted to investigate ongoing criminal conduct, such as gambling operations and narcotics distribution networks, and courts have consistently upheld applications and warrants which specify the targeted offenses by generic type, statutory designation, or both. Thus, for example, a narcotics wiretap can and should authorize interception of all conversations relating to narcotics, not merely those relating to a single, specific transaction.

b. "Specific person." Portions of Title III require the application and order to specify "the identity of the person, if known, whose communications are to be intercepted." Read in light of Berger and the Senate Judiciary Committee Report, these provisions seem to define the permissible scope of monitoring in terms of the targeted individuals as well as the specified crime and phone or location. If a judge issued an order that identified X as a probable narcotics trafficker and authorized a tap on X's phone, for example, a strict reading of the statute would lead one to


128 See supra note 91.


believe that the investigators would be empowered to "search" X's conversations, and only X's conversations, over that phone for evidence relating to narcotics offenses. Several Supreme Court decisions, however, have substantially reduced the significance of the identification provisions, thereby broadening considerably what and who the agents monitoring a tap or bug may listen to.

The first such decision was *United States v. Kahn*, in which FBI agents obtained a court order authorizing the interception of bookmaking-related conversations "of Irving Kahn and others, as yet unknown," over Kahn's home phone. The next day investigators intercepted Kahn's wife making two phone calls to another gambler. These conversations were suppressed prior to trial and the Seventh Circuit affirmed on appeal, reasoning that the wiretap order permitted interception only when Irving Kahn was a party to the conversation. The Supreme Court reversed, stressing that the interception order authorized interception of conversations "of Irving Kahn and others," not just conversations "between Irving Kahn and others." Since a primary purpose of the court order was to identify and gather evidence against Kahn's confederates, the Court concluded that Kahn himself need not be a party to a conversation for it to be lawfully intercepted.

The *Kahn* decision dramatically reduced the significance of the Title III identification provisions. A wiretap is no longer consid-

---

135 Id. at 196.
136 *Kahn*, 415 U.S. at 156.
137 Id. at 156-57. For an inciteful critique of this aspect of *Kahn*, see Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 88-93 (1983). The Court analogized to a search warrant for physical evidence, and quoted a Second Circuit case with approval: "The Fourth Amendment requires a warrant to describe only 'the place to be searched, and the persons or things to be seized,' not the persons from whom things will be seized." *Kahn*, 415 U.S. at 155 n.15 (quoting United States v. Fiorella, 468 F.2d 688, 691 (2d Cir. 1972) (quoting U.S. CONST. amend. IV), *cert. denied, 417 U.S. 917 (1974)*) . The logic is flawed for the simple reason that the analogy is flawed. See *supra* note 11; Goldsmith, *supra*.
138 The Court noted that Title III only requires the naming of a person in the application or order "if known," *United States v. Kahn*, 415 U.S. 143, 157 (1973), and only if there is probable cause to believe that the individual is "committing
ered a warrant authorizing a "search" of the identified suspect's conversations. Rather, the court order authorizes a "search" of the telephone itself and of all conversations through that telephone, regardless of who the participants of any particular conversation might be.\textsuperscript{139}

Later the same year, in two decisions not directly related to the identification provisions but affecting their significance, the Court concluded that a failure by the government to comply with a provision of Title III does not always render the interception of communications "unlawful" and therefore subject to suppression.\textsuperscript{140} Rather, if a defendant can establish that a Title III provision has been violated, a court must then assess whether that provision is one of those which "directly and substantially implement the congressional intention to limit the use of intercept procedures."\textsuperscript{141} If

the offense." \textit{Id.} at 155. \textit{See also} 18 U.S.C. §§ 2518(1)(b)(iv), (4)(a) (1982 & Supp. IV 1986) (quoted language). The majority found that when there is probable cause to believe that a particular telephone is being used to commit an offense, but no particular person is identifiable, the order may properly issue without naming any specific party at all. \textit{Id.} at 157.

\textsuperscript{139} This is so, of course, only if the goals of the wiretap or eavesdrop include identifying other participants in the criminal scheme, and only if the court order is worded in terms of communications "of X and others," rather than "of X with others." Since the Kahn decision, identification of other participants should be a stated goal of every properly drafted application under Title III or its state equivalents, and virtually every interception order has contained the words "conversations of X and others." See, e.g., \textbf{UNITED STATES ATTORNEYS' MANUAL}, Title 9—Criminal Division § 9-7.921 (Standard Form Interception Order), ch. 7, p. 821 (1985).

This is also not to suggest that agents may ignore the statutory directive to "minimize" the interception of non-pertinent conversations. See 18 U.S.C. § 2518(5) (Supp. IV 1986). Minimization is discussed at \textit{infra} notes 150-58 and accompanying text.

\textsuperscript{140} United States v. Chavez, 416 U.S. 562, 574-75 (1974); United States v. Giordano, 416 U.S. 505, 527 (1974). In \textit{Giordano}, the application for the intercept order was not authorized by any of the officials specified in 18 U.S.C. § 2516(1) (Supp. IV 1986), but by the Attorney General's Executive Assistant. \textit{Giordano}, 416 U.S. at 509-10. The issuing judge authorized the interceptions because they were accompanied by letters bearing the signatures of a specially-designated Assistant Attorney General, but the special designee had not reviewed the applications and someone in his office had affixed the signatures. \textit{Id.} In \textit{Chavez}, a proper official had authorized each application, satisfying § 2516(1), but the memo sent back to the agent applying for the warrant named a different official, resulting in a violation of 18 U.S.C. § 2518(1)(a) (1982), which requires identification of the authorizing officer.

\textsuperscript{141} \textit{Chavez}, 416 U.S. at 575 (quoting \textit{Giordano}); \textit{Giordano}, 416 U.S. at 527.
the provision does not meet this test, suppression will not follow.\footnote{429 U.S. 413 (1977).} Three years later, in \textit{United States v. Donovan},\footnote{429 U.S. 413 (1977).} the Court applied this test directly to the statutory identification provisions. Even though it rejected the government's argument that Title III only requires the application to list the "principal target" of the investigation,\footnote{Donovan, 429 U.S. at 423-28.} and found that the government had failed to comply with the identification provisions,\footnote{Id. at 432.} the Court held that these provisions do not play a "substantive role" with respect to judicial authorization of intercept orders.\footnote{The issue as stated by the Court was "whether the identification in an intercept application of all those likely to be overheard in incriminating conversations plays a 'substantive role' with respect to judicial authorization of intercept orders . . . ." \textit{Id.} at 435-37. The Court found nothing in the legislative history to suggest that the identification requirements played a "a central, or even functional, role in guarding against unwarranted use of wiretapping or electronic surveillance." \textit{Id.} at 437. (quoting United States \textit{v.} Chavez, 416 U.S. 562, 578 (1974)).} Hence, failure to properly identify some suspects did not render the interception order invalid and did not require suppression of intercepted conversations.\footnote{Id. at 435-37. The Court added that a different result might have been reached if the authorities had deliberately failed to identify certain individuals in an application in order to mislead the judge. \textit{Id.} at 436 n.23. The Court also}

In \textit{Giordano}, the Court concluded that the provision specifying the officials who may authorize applications, 18 U.S.C. § 2516(1) (Supp. IV 1986), was "intended to play a central role in the statutory scheme and that suppression must follow when it is shown that this statutory requirement has been ignored." \textit{Giordano}, 416 U.S. at 528. The issue was decided correctly in light of the legislative intent. \textit{See supra} note 112 and accompanying text. For a critique of \textit{Giordano}, see Goldsmith, \textit{supra} note 137; at 76-85.

Conversely, in \textit{Chavez}, the Court concluded that the provision requiring identification in the application of the official who authorized the application, 18 U.S.C. § 2518(1)(a) (1982), had "[n]o role more significant than a reporting function," \textit{Chavez}, 416 U.S. at 579. Thus, so long as a properly empowered official has given authorization, the application and order are valid, and the interceptions lawful, even if another official has been incorrectly named in the application and order.

\begin{thebibliography}{9}
\bibitem{1} \textit{Chavez}, 416 U.S. at 579-80.
\bibitem{2} \textit{Donovan}, 429 U.S. 413 (1977). In \textit{Donovan}, government agents learned during the course of a wiretap that certain parties were discussing illegal gambling activities with the original targets of the intercept order, but the agents failed to name the parties along with others when they applied for an extension of the initial order. \textit{Id.} at 419. The district court suppressed all evidence gathered against these defendants under the order and the Sixth Circuit affirmed. \textit{Id.} at 421.
\end{thebibliography}
As a result of *Kahn* and *Donovan*, the identification provisions now serve only lesser purposes in the typical Title III interception order.\(^{148}\) They do not play a significant role in limiting the scope of what and who the monitoring agents can listen to once they obtain the court order.\(^{149}\)

## B. Execution of an Intercept Order: the Minimization Provision

Legislative guidance for executing an order consists primarily of a single sentence in Title III:

> Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.\(^{150}\)

Although some uncertainty exists about how to assess whether investigators have complied with this "minimization" provision,\(^{151}\) it clearly requires some attempt to avoid listening to or recording conversations that are not particularly described in the order. The provision does not require the monitoring agents to eliminate the interception of non-pertinent conversations altogether, because the agents cannot know, until a conversation is over, what the conversants will say to each other. On the other hand, it would be improper to routinely intercept every conversation that occurs over the tapped telephone or within the bugged location. One widely

---

\(^{148}\) Identification of all those likely to be intercepted helps alert the issuing judge to the scope of the investigation, ensures fulfillment of the obligation to inform the judge of prior applications, 18 U.S.C. § 2518(1)(e) (Supp. IV 1986), and triggers the mandatory service of post-interception notice and inventory. 18 U.S.C. § 2518(8)(d) (1982 & Supp. IV 1986).

\(^{149}\) The identification provisions have greater significance with regard to roving intercept orders. See infra notes 219-27 and accompanying text.


approved partial solution to this dilemma is "spot-monitoring." When a particular conversation appears to be non-pertinent but the monitoring agent is unsure that it will remain so, he turns the monitoring equipment off but resumes monitoring a minute or two later, and he repeats the process until the conversation either ends or turns to matters that are pertinent to the investigation.152

In Scott v. United States,153 the Supreme Court considered how compliance with the minimization provision should be assessed. The Court held that the monitoring agents' conduct must be evaluated under a standard of objective reasonableness, without regard to the intent or motivation of the agents involved.154 Thus, if the facts and circumstances render minimization difficult or impossible, even failure to make any attempt to minimize is not a violation.155 Moreover, at least when investigators have reasonable cause to believe they are probing a complex conspiracy involving a large number of participants, it is permissible for monitors to listen to and record all conversations until they have had "an opportunity to develop a category of innocent calls."156

After Scott, the minimization provision often provides only a limited check on the broadened scope of monitoring permitted as

---

152 See, e.g., United States v. Clerkley, 556 F.2d 709, 717 (4th Cir. 1977) (approving spot-monitoring of calls), cert. denied, 436 U.S. 930 (1978); United States v. Hinton, 543 F.2d 1002, 1011-12 (2d Cir.) (approving a five-minute "ascertainment period" to spot-check telephone calls, where code language was being used and many of the calls eventually became narcotics related), cert. denied, 429 U.S. 980 (1976); United States v. Losing, 539 F.2d 1174, 1180-81 (8th Cir. 1976) (finding spot-checking permissible), cert. denied, 434 U.S. 969 (1977); United States v. Costello, 610 F. Supp. 1450, 1477 (N.D. Ill. 1985) (agents may spot-check to determine whether subject of conversation has shifted), aff'd mem., sub nom. United States v. Olson, 830 F.2d 195 (7th Cir. 1987); United States v. Clemente, 482 F. Supp. 102, 108-10 (S.D.N.Y. 1979) (approving a spot-monitoring procedure in which two minutes of monitoring was followed by one minute off), aff'd mem., 633 F.2d 207 (2d Cir. 1980); State v. Catania, 85 N.J. 418, 446, 427 A.2d 537, 551 (1981) (spot-monitoring is an effective method); People v Floyd, 41 N.Y.2d 245, 251, 360 N.E.2d 935, 941, 392 N.Y.S.2d 257, 263 (1976) (upholding procedure in which monitoring intervals of 30 to 40 seconds were used).


154 Id. at 137-39. The Court found that this was the appropriate standard under Title III and under the Fourth Amendment. Id.

155 In Scott, the district court found that the agents "made no attempt to comply" with the minimization provision. Id. at 133.

156 Id. at 142.
a result of Kahn and Donovan.\textsuperscript{157} Although the Justice Department has not ignored the statutory mandate to minimize interception of non-pertinent conversations,\textsuperscript{158} it is no overstatement that there are few significant restrictions on what the agents may listen to when executing a typical Title III wiretap or eavesdrop order.

III. THE "EMERGENCY SURVEILLANCE" PROVISION

A. Interpretation and Application of the Requirements

Legislative regulation of emergency electronic surveillance can take one of three approaches: prohibition of such surveillance altogether, exclusion of such surveillance from the scope of the statute, or specification of the circumstances under which such surveillance may be conducted. When Congress enacted Title III, it attempted to follow the third approach. The provision governing emergency surveillance, section 2518(7),\textsuperscript{159} has significant flaws, however, and the Justice Department's policy with regard to such surveillance has been extremely, and perhaps excessively, cautious.\textsuperscript{160} As a result, the provision has been invoked only rarely, and there has been virtually no judicial discussion or interpretation of it.

In essence, the emergency surveillance provision\textsuperscript{161} spells out five requirements which must be satisfied if emergency nonwarrant sur-

\textsuperscript{157} See supra notes 133-49 and accompanying text.
\textsuperscript{158} In almost every reported federal case discussing minimization, the courts have emphasized that the agents complied with the provision. See, e.g., United States v. Lawson, 780 F.2d 535, 540 (6th Cir. 1985); United States v. Dorfman, 542 F. Supp. 345, 390-98 (N.D. Ill.), aff'd in part and rev'd in part on other grounds, 690 F.2d 1217, 1230 (7th Cir. 1982); United States v. Susquet, 547 F. Supp. 1034, 1045-47 (N.D. Ill. 1982); United States v. Loften, 518 F. Supp. 839, 843-45 (S.D.N.Y. 1981). See also supra note 152 (cases cited therein).
\textsuperscript{159} 18 U.S.C. § 2518(7) (Supp. IV 1986).
\textsuperscript{160} See infra notes 205-09 and accompanying text.

Notwithstanding any other provision of [Title III], any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, or the Associate Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that —
veillance is to be lawful: (1) the factual basis for a standard intercept order must exist, (2) there must be an "emergency situation," (3) the emergency must fit within a statutorily recognized category, (4) an eligible official must give advance authorization for the interception, and (5) a retroactive court order must be obtained within forty-eight hours approving the interception. Problems of interpretation or application exist with regard to several of these requirements.

1. Grounds for an order. Even though the emergency surveillance provision does not require a pre-interception court order, all of the requirements for such an order must exist at the time the surveillance commences. In other words, there must be adequate probable cause, the crime involved must be one of the offenses designated by the statute, there must be a valid basis for belief that other investigative procedures have been or would be unavailing or too dangerous, and other requirements must be met. In general, therefore, judicial interpretation of these requirements should apply equally well to the emergency context.

(a) an emergency situation exists that involves —
   (i) immediate danger of death or serious physical injury to any person,
   (ii) conspiratorial activities threatening the national security interest, or
   (iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and
(b) there are grounds upon which an order could be entered under [Title III] to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with [§ 2518] within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and [notice of such interceptions] shall be served on the person named in the application.

162 The statutory requirements for an interception order are discussed in supra notes 108-23 and accompanying text.
2. "Emergency situation." Although Title III does not define this term, the Senate Judiciary Committee Report on the statute states:

Often in criminal investigations a meeting will be set up and the place finally chosen almost simultaneously. Requiring a court order in these situations would be tantamount to failing to authorize the surveillance. The provision reflects existing search warrant law in which the principle of emergency search is well established. This passage can be read as expressing Congressional intent that an "emergency situation" will be found to exist whenever there are grounds for an interception order, and there is good reason to believe that a crime-related meeting or phone conversation will occur before an interception order can be obtained. This definition of "emergency situation" appears broader than is advisable or even, perhaps, constitutional. Hence, Congress limited the types of emergencies in which the provision may be invoked.

3. **Factual settings in which emergency surveillance is permitted.** Aside from threats to national security, the emergency surveillance provision applies only in situations involving "immediate danger of death or serious physical injury to any person," or

---

163 S. REP. No. 1097, 90th Cong., 2d Sess. 104 (citing Carroll v. United States, 267 U.S. 132 (1925); Schmerber v. California, 384 U.S. 757 (1966)), reprinted in 1968 U.S. CODE CONG. & ADN. NEWS 2112, 2193. In Carroll, the Court held for the first time that if a police officer has probable cause to believe that an automobile being driven on the public highways contains contraband, he may stop it and conduct a search of it without first obtaining a warrant. *Carroll*, 267 U.S. at 155-56. Among other reasons, the Court emphasized that the automobile might leave the jurisdiction or be emptied of the contraband by the time the officer could obtain a warrant. *Id.* at 146. *Schmerber* is discussed at *supra* notes 40-42 and accompanying text.

164 *See supra* notes 90-91 and accompanying text. Presumably, this is why Congress chose to restrict such surveillance to "organized crime" investigations. *See supra* notes 172-75 and accompanying text.


"conspiratorial activities characteristic of organized crime." The former is referred to below as the "immediate danger clause," and the latter as the "organized crime clause."

a. The immediate danger clause. Surprisingly, until amended in 1984, section 2518(7) had not explicitly authorized emergency surveillance in life-threatening situations. Such surveillance was lawful only if the Justice Department could rationally conclude that the conduct in question fit within the organized crime clause. As a result, on at least a few occasions law enforcement officials decided that they could not lawfully conduct surveillance even where such surveillance would have assisted efforts to protect or rescue a victim. The 1984 amendment to section 2518(7) thus filled an appalling gap in Title III.

The report of the Senate committee that drafted the amendment spells out the intended scope of the immediate danger clause:

The type of situations intended to be included within this exception generally would relate to those involving the taking of a hostage, the kidnapping of a victim, or the planning of an execution. These and similar situations involve serious and immediate threats to the life of innocent victims, and the use of electronic surveillance would focus more on the prevention of serious injury or death to that victim than it would on the collection of evidence which would be of secondary importance at the time.

The immediate danger clause is likely to cause few problems of interpretation, although some circumstances can be imagined in which the required degree of immediacy or danger is in doubt.

167 Id. § 2518(7)(a)(iii).
168 See Wiretap Amendments, Hearings Before the Subcommittee on Criminal Justice of the Committee on the Judiciary, United States Senate, 96th Cong., 2d Sess. 17-19 (1980) (prepared statement of L. Colewell, Executive Assistant Director, Federal Bureau of Investigation) [hereinafter Wiretap Hearings]. These hearings were held to discuss an earlier attempt to add an "immediate danger" clause to § 2518(7); although passed in the Senate by voice vote, it died for lack of action in the House. See S. REP. No. 225, 98th Cong., 2d Sess. 394 n.3, reprinted in 1984 U.S. CODE CONG. & ADMIN. NEWS 3182, 3533.
170 Suppose, for example, the authorities learn of an assassination that will be
b. The organized crime clause. Although this clause has been part of Title III since its original enactment in 1968, it has almost never been invoked.\textsuperscript{172} One reason for the clause's dormance may be its vagueness. Neither Title III nor its legislative history offer any definition of "organized crime" or of "conspiratorial activities characteristic of" it.

Congress did, however, include a definition of "organized crime" in a different section of the Act in which Title III appears: ""Organized crime' means the unlawful activities of the members of a highly organized, disciplined association engaged in supplying illegal goods and services, including but not limited to gambling, prostitution, loan sharking, narcotics, labor racketeering, and other unlawful activities of members of such organizations."\textsuperscript{173} This definition and the title of which it was a part have been since repealed.\textsuperscript{174} Whether it ever applied or might still apply to the Title III emergency surveillance provision, or clarifies it to any significant extent is, of course, open to debate.\textsuperscript{175}

---

\textsuperscript{171} Suppose the authorities learn of a plan to rob a bank the next day and have an opportunity to eavesdrop upon two or more of the plotters to learn the particulars, including the identity of the targeted bank. There is no reason to suspect that the robbers intend to kill or injure anyone, but armed robberies are inherently dangerous to human life and health. Although the statute speaks less clearly than might be desired, emergency surveillance certainly would be eminently reasonable under these circumstances.

\textsuperscript{172} In 1980, spokesmen for the Justice Department and the Federal Bureau of Investigation reported to the Senate Judiciary Committee that the provision had been invoked only in life-threatening situations. See Wiretap Hearings, supra note 168, at 7 (Testimony of Phillip B. Heymann, Assistant Attorney General, Criminal Division); \textit{id.} at 11 (prepared statement of Mr. Heymann). Apparently this is still Department policy. See \textit{infra} notes 205-07 and accompanying text.


\textsuperscript{175} A few state courts have applied this definition, but their decisions provide
4. **Pre-interception authorization.** Emergency surveillance is lawful only if authorized by the United States Attorney General, the Deputy Attorney General, or the Associate Attorney General.¹⁷⁶ Until the 1984 amendment to section 2518(7),¹⁷⁷ only the Attorney General was empowered to authorize such surveillance. In all likelihood, the difficulty in obtaining the immediate attention of one of only three officials in the entire Department of Justice discourages investigators from even seeking approval for emergency surveillance.

5. **Post-interception authorization.** Within forty-eight hours of the commencement of interception, the officials conducting the interception must submit an application to a judge seeking an order approving of the surveillance.¹⁷⁸ In deciding whether to issue such an order, the judge to whom the application is submitted must determine whether the application complies with all other aspects of Title III,¹⁷⁹ and must also determine whether the pre-application situation truly qualified as an "emergency."¹⁸⁰ To date, no reported little guidance on its application generally. See Shingleton v. State, 39 Md. App. 527, 535-36, 387 A.2d 1134, 1139 (1978) (conspiracy among three persons to distribute cocaine did not constitute "organized crime"; interceptions suppressed); Commonwealth v. Thorpe, 384 Mass. 271, 281, 424 N.E.2d 250, 255-56 (1981) (where individual offering to sell an upcoming police promotion examination claimed to be part of an "organization," sufficient nexus to organized crime was shown to justify non-warrant consensual surveillance which is permissible in Massachusetts only to investigate "organized crime"); Commonwealth v. Jarabek, 384 Mass. 293, 296, 424 N.E.2d 491, 493 (1981) (a scheme by two municipal officials to extort a kickback from a single contractor did not create a reasonable suspicion that organized crime was involved; consensual interception suppressed); State v. Nobozny, 54 Ohio St. 2d 195, 207-08, 375 N.E.2d 784, 793 (1978) (participation of at least three individuals in a kidnapping was sufficiently characteristic of "organized crime"; emergency interceptions were properly admitted in subsequent murder trial). Thorpe and Jarabek are discussed in Note, Relaxing the Organized Crime Requirement for Electronic Surveillance: A Carte Blanche for the "Uninvited Ear"? 5 W. NEW ENG. L. REV. 725 (1983).

¹⁷⁶ 18 U.S.C. § 2518(7) (Supp. IV 1986). The principal prosecuting attorney of a state or subdivision thereof may also authorize it in pursuance of a state statute. *Id.*


¹⁷⁹ See *id.* § 2518(7)(b).

¹⁸⁰ Neither Title III, the Senate report on Title III, nor the Senate reports on
federal case addresses any of the issues outlined in this paragraph.

**B. Justice Department Policies and Practices**

To properly evaluate the Title III emergency surveillance provision, it is necessary to understand the practices and policies the Justice Department follows in invoking the provision. Since these policies and practices are best understood in the context of the Department's normal procedures for processing Title III applications, however, it is to that subject that we first turn.

1. **The application authorization process.** Before a government attorney or investigator may apply to a judge for an interception order, he or she must be authorized to do so by one of only a few authorizing officials at the Department of Justice. As might be expected, the decision to employ so potentially intrusive and expensive an investigative technique is reviewed at the local level before it ever reaches the Justice Department. This local review is, as a rule, conducted both by the special agent in charge of the field office of the applicable investigative agency and by the United States Attorney's Office or the federal Strike Force Attorney whose

the 1984 and 1986 amendments to 18 U.S.C. § 2518(7) specifically require a judge to assess the adequacy of the emergency in deciding whether to issue an order of approval. Nevertheless, a judicial responsibility to do so is implicit in the "exigent circumstances" exception to the Fourth Amendment warrant requirement, and Congress intended to codify this exception with regard to interception of communications when it enacted Title III. See S. REP. No. 1097, 90th Cong., 2d Sess 104, reprinted in 1968 U.S. CODE CONG. & ADNM. NEWS 2112, 2193.

181 Unless otherwise noted, the information contained in this section is based on discussions in 1985 and 1987 with Frederick Hess and Maureen Killian, the Director and Senior Attorney, respectively, of the Office of Enforcement Operations, United States Department of Justice. One of the primary functions of the Office of Enforcement Operations is to review and evaluate all Title III applications before they are submitted to a statutorily designated official for approval.

182 Authorizing officials include the Attorney General, Deputy Attorney General, Associate Attorney General, or an Assistant Attorney General whom the Attorney General has specially designated. 18 U.S.C. § 2516(1) (1982 & Supp. IV 1986). See supra note 112 and accompanying text. Until this provision was amended in 1984, only the Attorney General or a specially designated Assistant Attorney General could authorize applications.

183 The applicable investigative agency is usually the Federal Bureau of Investigation ["FBI"] or the Drug Enforcement Agency ["DEA"]. Thereafter it is submitted to the agency's headquarters in Washington for further review.
geographical jurisdiction includes the targeted telephone or premises.\textsuperscript{184}

How long does this local review process take? The only accurate generalization is that it varies depending on the case,\textsuperscript{185} the agency, the region, and the United States Attorney’s Office. Department of Justice officials in Washington estimate that, on the average, the review process on the local and regional level takes three to four weeks.\textsuperscript{186}

The main document in the application is an affidavit, usually submitted by an investigator,\textsuperscript{187} which is drafted to supply all of the information required by Title III. The affidavit must, among other things,\textsuperscript{188} specify the targeted premises or telephone,\textsuperscript{189} identify the targets of the intercept, if known,\textsuperscript{190} provide details of the investigation to date, demonstrating probable cause to believe that conversations relating to specific crimes will be intercepted over the phone or in the premises in question,\textsuperscript{191} and further demonstrating that ordinary investigative techniques have been tried and have failed, or would not succeed if tried, or would be too dangerous.\textsuperscript{192} If a particular application is the first to be used in an investigation, merely drafting the affidavit is likely to take several days.\textsuperscript{193}

\textsuperscript{184} The special agent in charge of the investigative agency’s field office and the United States Attorney each apparently has veto power. The United States Attorneys’ Manual directs, for example, that it is incumbent upon any United States Attorney in whose district an application for a Title III interception order is to be filed to evaluate personally the merits of the proposed application prior to its submission to the Department of Justice for filing authorization. A United States Attorney should not authorize the submission of any application unless, in his judgment, the interception would foster the interests of justice. He should not approve an authorization request solely because an investigative agency strongly urges it. \textit{United States Attorneys’ Manual}, tit. 9, ch. 7, at 12-12a (1985).

\textsuperscript{185} Some investigations might require months to acquire probable cause to tap or bug a particular telephone or premises.

\textsuperscript{186} \textit{See supra} note 181.

\textsuperscript{187} The investigator is usually an FBI or DEA agent or, less frequently, a government attorney.

\textsuperscript{188} For a more detailed summary of what a Title III application must contain, see \textit{supra} notes 108-49 and accompanying text.


\textsuperscript{190} \textit{Id.} § 2518(1)(b)(iv).

\textsuperscript{191} \textit{Id.} § 2518(1)(b); 18 U.S.C. §§ 2518(3)(a),(b),(d) (1982 & Supp. IV 1986).

\textsuperscript{192} 18 U.S.C. §§ 2518(1)(c), (3)(a) (1982).

\textsuperscript{193} This, at least, was my own experience as a prosecutor in the New York
In addition to the affidavit, the application package contains the application itself and a draft of the interception order. If the U.S. Attorney and the investigative agency’s special agent both approve the interception application package, it is then sent to Washington, usually by courier or express mail. Once again, it is subject to a dual review process by both the Justice Department attorneys and the investigative agency.

Within the Justice Department, all Title III application packages are referred to the Criminal Division’s Office of Enforcement Operations [“OEO”]. The director of OEO reviews each of the documents, sends a copy of the affidavit to the appropriate litigating section in the Criminal Division, and assigns the matter to one of OEO’s attorneys. The OEO attorney examines the application to determine whether the affidavit and proposed order comply with Title III and Justice Department standards.

When this examination is complete, the OEO attorney prepares a memorandum summarizing the application. This memorandum consists of: (a) a list of the premises and telephones in question, (b) a brief biography of the intended interceptees, (c) a statement as to whether any of the individuals, telephones or premises specified in the application have been the targets of prior interception applications, (d) a summary of the body of the application, out-

County District Attorney’s Office and New York City’s Special Narcotics Prosecutor’s Office (1969-1977). The typical affidavit in a federal Title III application is 30 to 50 pages long.

The sections are Narcotics, Organized Crime, and Public Integrity. The primary purpose for section review is to obtain an assessment of whether the investigation in which the proposed intercept will occur is important enough to merit the use of wiretapping or eavesdropping, although on occasion the sections also alert OEO to potential legal problems. As a rule, the section evaluations are returned to OEO within one or two days after the matter was referred to them.

Approximately 60% of federal Title III applications currently focus on narcotics trafficking. Most of the rest fall within the organized crime or public integrity categories. On rare occasions, a Title III order is sought to investigate criminal conduct relating to the nation’s internal security, but most surveillance for this purpose is conducted pursuant to FISA, supra note 165. For a detailed discussion of FISA, see C. Fishman, supra note 12, §§ 348-80.

Each application must contain “a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application . . . .” 18 U.S.C. § 2518(1)(e) (Supp. IV 1986). Because the individual authorizing the application is a Justice Department official, the required statement about prior applications is compiled by the Justice Department after a computer check of its Title III files.
lining probable cause and the particulars of the offenses being investigated, (e) an evaluation of the application's discussion of alternate procedures, (f) a brief discussion of minimization,\(^{196}\) and (g) a recommendation as to whether the application should be submitted to an authorizing official. The memorandum is reviewed by the director of OEO, who then submits it, together with the application, affidavit and order, a memorandum from the investigative agency,\(^{197}\) a memorandum from the Criminal Division litigating section, and other documents,\(^{198}\) to the authorizing official.\(^{199}\)

OEO officials estimate that it takes them approximately three to five days to review and approve a typical application, assuming it measures up to standards.\(^{200}\) If an affidavit is weak in one or more respects, approval is withheld until the OEO is satisfied. OEO officials are reluctant to approve an application where the probable cause showing is marginal, for example, or where there is concern that the probable cause showing is stale.\(^{201}\) It is not unusual for the OEO attorney to confer frequently by telephone with the in-

\(^{196}\) Minimization is discussed supra in notes 150-58 and accompanying text.

\(^{197}\) The investigative agency memorandum is usually a page or so in length. The director of OEO estimated that 85% of Title III applications involve the FBI and that the DEA is the enforcement agency in most of the rest. Within the FBI, each application is examined both by the Legal Counsel Division and the Criminal Division.

\(^{198}\) These consist of a memorandum signed by the authorizing official authorizing submission of the application to a judge, and other memoranda informing the applicant and the United States Attorney that they are authorized to submit the application to the judge.

\(^{199}\) The term “authorizing official” is defined at supra note 182.

\(^{200}\) The process can be compressed into several hours if a satisfactory affidavit application and proposed order have been prepared, see supra note 193 and accompanying text, if compelling circumstances exist and if the agents who will conduct the tap or bug can assure OEO that they are prepared and ready to do whatever is necessary technically to commence interception promptly once the order is issued.

\(^{201}\) “Generally, the Department expects the basic probable cause to be no more than 15 days old at the time the file containing the proposed affidavit, application and order are received by the Office of Enforcement Operations . . .,” United States Attorneys’ Manual, tit. 9, ch. 7, at 19 (1985). The probable cause showing can be updated, when necessary, by additional visual surveillance information from informers, or by using a “pen register.” A pen register is a device that records only the numbers dialed from a particular telephone and reveals no other information; therefore, pen registers are not regulated by Title III. United States v. New York Telephone Co., 434 U.S. 159, 170 (1977).
vestigative agent and government attorney who have drafted the documents, and who will supervise the investigation once the intercept order is issued, to clarify ambiguities in the papers and to discuss how possible shortcomings may be corrected. Once OEO approves an application, it usually must then hold the application in abeyance for another two or three days until the investigative agency has finished its own review.

For several reasons, the Justice Department routinely processes extensions\textsuperscript{202} more quickly than original requests. First, because litigation section officials have already determined that the investigation is important enough to merit the use of wiretapping or eavesdropping, there is no need to refer an extension to the various litigating sections. Second, the investigative agencies do not conduct their own review of extensions at headquarters level. Third, the probable cause showing for an extension usually consists primarily of excerpts of communications intercepted during the initial order, supplemented by descriptions of physical surveillance and other sources of information, and is therefore easier to analyze.

Whether the application relates to a new investigation or an extension, the final step in the process is the submission of application, affidavit, order, and accompanying documents and memoranda\textsuperscript{203} to an authorizing official. Most often, the official is the Assistant Attorney General in charge of the Criminal Division, who usually acts on the matter the same day he receives it.\textsuperscript{204} If

\textsuperscript{202} "Extension," as used here, is an interception order authorizing continued interception on an already existing tap or bug. Applications for a "second generation order," an order to tap or bug a new phone or premises based on information obtained from an ongoing tap or bug, are discussed at infra note 208-09 and accompanying text.

\textsuperscript{203} See supra notes 197-98 and accompanying text (discussion of memoranda).

\textsuperscript{204} The primary purpose for requiring an authorizing official's approval is to assure that a politically responsible official makes the policy judgment that the case at hand merits the use of wiretapping or eavesdropping. See supra note 112. Defendants seeking to suppress evidence obtained from wiretapping or eavesdropping occasionally seek to challenge the scope or nature of the authorizing official's review of the application. Courts have consistently held, however, that a statutorily-authorized official is entitled to what amounts to an irrebuttable presumption that he or she has exercised this authority properly, United States v. O'Malley, 764 F.2d 38, 40-41 (1st Cir. 1985); United States v. Todisco, 667 F.2d 255, 259 (2d Cir. 1981), cert. denied, 455 U.S. 906 (1983); United States v. Turner, 528 F.2d 143, 150-51 (9th Cir. 1975), cert. denied, 423 U.S. 996 (1976), and that it
the Assistant Attorney General of the Criminal Division is unavailable, or if that post is vacant, the application is usually submitted to another specially designated assistant attorney general, or on rare occasions to the Associate Attorney General.

2. Emergency Surveillance. The Justice Department has a straightforward policy concerning the Title III emergency surveillance provision: it does not approve pre-interception order surveillance except in life-threatening situations. Emergency surveillance is not authorized merely to gather evidence of criminal activity.

OEO officials gave several reasons for this policy. First, the requirements of the emergency provision are ambiguous, leaving enforcement officials uncertain about what it requires and what it permits. Second, OEO officials fear that the haste with which emergency applications must be handled creates an unacceptably high risk that mistakes will be made which will render the surveillance unlawful. Third, officials of the Justice Department are convinced that, except in life-threatening situations, emergency surveillance simply is not necessary.

is entirely proper for such an official to rely upon the summaries and recommendations of subordinates, United States ex rel. Machi v. United States Dep't of Probation & Parole, 536 F.2d 179, 184 (7th Cir. 1976) (application summarized for authorizing official by subordinate over telephone); United States v. Falcone, 505 F.2d 478, 481 (3d Cir. 1974), cert. denied, 420 U.S. 955 (1975) (telephone summary); United States v. Acon, 403 F. Supp. 1189, 1194-95 (W.D. Pa. 1975) (written summary).

Except as otherwise specified, the information in this section is based on conversations with Justice Department officials. See supra note 181.

See supra notes 172-75 and accompanying text. These uncertainties are aggravated by the lack of case law interpreting and applying the provision. Of course, if the Department had invoked the provision more frequently, it is likely that a body of case law discussing it would have developed by now.

It is particularly difficult, they insisted, to evaluate the factual basis for surveillance—probable cause to believe that specific individuals will use a specific telephone or premises to discuss specific crimes—based on a telephone conversation between OEO personnel and the government attorney or investigator who seeks approval of the surveillance. Problems multiply when, as is usually the case, the attorney or investigator is relating information obtained second- or third-hand from other investigators and informers concerning fast-breaking developments. Until the factual justification for an interception is committed to paper in an affidavit, OEO officials maintain, there is too great a risk that gaps in the needed factual showing may be overlooked. The problem is particularly acute, they said, because emergency surveillance requires them to deal with so fluid a factual situation: the information establishing probable cause is developing at the same time that they must evaluate the necessity for the interception.
It is not necessary to invoke the emergency provision when the need to tap a new phone or bug a new premises arises in the context of an ongoing Title III investigation, OEO officials maintain, because those conducting the investigation should be able to draft a new intercept application, affidavit and order for the new phone or premises in a matter of hours.\(^{203}\) OEO can process these papers, including review by a statutorily authorized official, within hours of when the papers are received.\(^{209}\) Nor is emergency surveillance truly necessary in situations not already involving a Title III intercept, OEO officials insist. Such situations arise only rarely, and are unlikely to pose "once-in-a-lifetime" opportunities. They feel it is better to follow established procedures, obtain an interception order, and be ready when the targets decide to transact their next deal.

Thus, the Justice Department has invoked the emergency surveillance provision of Title III only in life-threatening situations, about once a year over the last several years. Usually in such situations, the Attorney General discusses the need for such surveillance with the director of the investigative agency. If he decides that such surveillance is required, he authorizes the director to conduct the surveillance if the director determines that there is probable cause to do so. Then, as the statute requires, a law en-

\(^{203}\) Although an extension application must satisfy the same statutory requirements as an original or first generation application, as a practical matter the affidavit in a second generation application need not reproduce all of the information contained in the first generation application; it suffices to incorporate the prior affidavit by reference and attach a copy of it to the second generation application. Of course, the second generation application must demonstrate why normal investigative procedures have not or would not suffice. Compare United States v. Santora, 583 F.2d 453, 466-67 (9th Cir.), vacated on other grounds, 441 U.S. 939, suppression reaff’d after remand, 600 F.2d 1317, 1322 (1979) (failure to detail other procedures that had been employed to investigate targets of the new tap invalidated second generation order) with United States v. Williams, 580 F.2d 578, 588-90 (D.C. Cir. 1978) (length and complexity of investigation that preceded the first generation order, risk that ordinary procedures at new location might alert targets, and need to act quickly lest important opportunities be lost satisfied the other procedures requirement in second generation application) and United States v. O'Malley, 764 F.2d 38, 43-44 (1st Cir. 1985) (where targets of second generation applications were the same individuals who were targets of the first generation order, ordinary procedures showing for first generation order applied to second generation application as well).

\(^{209}\) This occurs about five to ten times a year.
forcement official applies to a judge for a retroactive order of approval within forty-eight hours of the commencement of interception.

IV. THE ROVING INTERCEPT PROVISION

The Electronic Communications Privacy Act of 1986 ["ECPA"] substantially revised the law of electronic communications and electronic surveillance. Among the most dramatic and significant provisions added to Title III by ECPA is the roving intercept provision. This provision creates an express exception in certain circumstances to the requirement that an application and order specify the telephone to be tapped or the location to be bugged.

210 Pub. L. No. 99-508, 100 Stat. 1848 (1986). The most dramatic impact of the ECPA is the creation of a new legal category, electronic communications, and provisions protecting the privacy, and regulating the interception, of such communications. See generally C. Fishman, supra note 12, §§ 7.21-7.70.


212 18 U.S.C. § 2518(1)(b)(ii) (Supp. IV 1986) requires that an application for an interception order must contain "a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted." Similarly, § 2518(3)(d) requires that before a judge issues an interception order, he or she must find that there is probable cause for belief that the facilities or the place targeted for interception are being used, or are about to be used, in connection with the commission of the offenses specified in the application, or are leased to, listed in the name of, or commonly used by the individuals targeted in the application.

The roving intercept provision says:

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(a) in the case of an application with respect to the interception of an oral communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(ii) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(iii) the judge finds that such specification is not practical; and

(b) in the case of an application with respect to a wire or electronic communication—

(i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney Gen-
In essence, the roving intercept provision provides that if federal investigators can show that specification of the particular place for interception of an oral communication is not practical, they may obtain an oral intercept order authorizing them to intercept all of their suspect's face-to-face conversations relating to the crime under investigation, no matter where those conversations happen to occur. Similarly, if federal investigators can show that a suspect is changing telephones with the purpose of thwarting interception, they may obtain an intercept order authorizing them to intercept all of their suspect's telephone conversations relating to the crime under investigation, no matter what telephone he uses.

The application and order are the same, in most respects, for a roving intercept as they are for a standard wiretap or oral intercept. In some respects, however, the requirements for a roving interception order differ significantly from those that apply to other Title III applications and orders. The discussion below explains the additional requirements that must be satisfied before investigators may obtain a roving intercept order, the special issues that arise when such an order is being used, and the provision's constitutional validity.

A. Application and Order: Additional Requirements

To obtain a roving intercept order, investigators must satisfy the standard Title III requirements and, in addition, must identify the intended interceptee, make a special showing of need to justify waiving the particular location or facilities requirement, and "particularly describe" the sought-after conversations in ways that differ from a standard intercept order. Moreover, fewer Justice Depart-
ment officials are empowered to authorize a roving intercept application than are empowered to authorize a standard intercept order application.

1. Authorization for application. The list of officials who may authorize a roving intercept application is similar to the list of those who may authorize standard Title III intercept applications, with the notable exception that "any Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General" may authorize a standard, but not a roving, intercept.\(^{216}\) Although the legislative history of ECPA contains no explicit explanation for this more "limited list"\(^ {217}\) of authorizing officials, the reason is obvious enough. A roving tap or bug is potentially far more intrusive into privacy than a standard interception order, so it is even more important to centralize the policy decisions in a "publicly responsible official subject to the political process."\(^ {218}\)

2. Identity of intended interceptee. In essence, in the roving intercept provision, Congress has substituted particularity of the interceptee's identity for particularity of the facilities or location of the intercept. A standard Title III application and order must include "the identity of the person, if known, committing the offense and whose communications are to be intercepted."\(^ {219}\) As this phrase has been interpreted by the Supreme Court, once investigators obtain a standard wiretap or oral intercept order, they may listen to any conversation that occurs on the targeted phone or location, even if none of the participants in the conversation has been previously identified as a suspect in criminal conduct, even, that is, if all the conversants are "unknowns,"\(^ {220}\) so long as they comply with the mandate to minimize the interception of communications that are not pertinent to the investigation.\(^ {221}\) By contrast, under the

---


\(^ {220}\) See supra notes 130-49 and accompanying text.

\(^ {221}\) Minimization is discussed in supra notes 150-58 and accompanying text.
roving intercept provision, an oral, wire or electronic intercept application is sufficient only if it "identifies the person believed to be committing the offense and whose communications are to be intercepted..." The omission of the phrase "if known" from the roving intercept provision, although not explicitly discussed in the reports of either the Senate or House Judiciary Committees, is obviously intended to limit the availability and use of these intercepts.

Roving intercept orders are permissible only when the application demonstrates that a particular identified individual or individuals can be expected to use numerous telephones or locations to discuss their crimes as a means of evading surveillance. This more demanding identification requirement precludes investigators from using a roving intercept order as authority to intercept communications between two "unknowns."

The question remains: how fully must a roving intercept application and order "identify" the interceptee? Neither the statute nor the legislative history provides an answer. It is unlikely, however, that Congress intended to insist that the application necessarily contain the interceptee's true name, date of birth, permanent address, and occupation. The likely targets of a roving intercept—organized criminals, sophisticated narcotics traffickers, terrorists, and

Minimization of roving intercepts is discussed in infra notes 270-76 and accompanying text.


224 There is also a quirk in the language of these subsections that is not explained in the Senate Report and for which I can fathom no reason. A roving oral intercept order is permitted if, among other things, the application "identifies the person committing the offense and whose communications are to be intercepted..." 18 U.S.C. § 2518(11)(a)(ii) (Supp. IV 1986) (emphasis added). A roving wiretap or electronic intercept is permitted if, among other things, the application "identifies the person believed to be committing the offense and whose communications are to be intercepted..." 18 U.S.C. § 2518(11)(b)(ii) (Supp. IV 1986) (emphasis added). Presumably, probable cause to believe that the person is committing the offense under investigation would be required, and would be sufficient, to satisfy either provision.

225 This will be discussed in more detail at infra notes 228-42 and accompanying text.
the like—often use multiple aliases and lead lives of dissembling for the very purpose of frustrating attempts by investigators to fully identify them. It should suffice if the application and order contain enough identifying information so that the judge can be confident the agents know to whom they are allowed to listen.

3. Showing of need. Both the oral and wiretap subdivisions of section 2518(11) require an application to include a showing of special need to obtain a roving intercept order. The special showing provisions differ somewhat, however, and it seems probable from the legislative materials and circumstances surrounding the enactment of the statute that a lesser showing of need is required for a roving oral intercept order than for a roving wiretap or electronic communication intercept order.

An application for a roving oral intercept order must contain "a full and complete statement as to why [specification of the facilities from which, or the place where, communications are to be intercepted] is not practical," and the order may only be issued if "the judge finds that such specification is not practical . . . ." A Senate Judiciary Committee report observes that "[s]ituations where ordinary specification rules would not be practical would include those where a suspect moves from room to room in a hotel to avoid a bug or where a suspect sets up a meeting with another suspect on a beach or a field." This comment is useful to a point, but still leaves unanswered many questions concerning the scope of the oral roving intercept provision and the type of showing required to satisfy it.

The simplest example of the need for a roving oral intercept order is what might be called the "single meeting scenario." Assume that investigators learn that X, the target of an ongoing investigation, plans to meet within a few days with Y to finalize

---

227 Such information might include nicknames, physical descriptions, and the like.
228 Subdivision (a) governs oral communications, and subdivision (b) governs wire or electronic communications. 18 U.S.C. § 2518(11)(a), (b) (Supp. IV 1986).
the details of a crime they have been discussing, but that the location for the meeting will not be set until just a few hours before it is to take place. Until the enactment of section 2518(11) in 1986, law enforcement officials in this situation were forced to wait until they had probable cause to believe they knew where X and Y would meet before applying for a court order authorizing them to bug that particular location.231 As a practical matter it was often impossible to complete the application process and submit the application to a judge until long after the meeting had taken place.232 18 U.S.C. § 2518(11)(a) clearly permits the agents to obtain an intercept order as soon as they learn that the meeting will occur, even though they do not yet know where.233

The issue of scope arises when more than merely one-time surveillance of one-of-a-kind meetings is involved. Title III permits judges to issue standard, non-roving interception orders of up to thirty days' duration.234 Had Congress intended a shorter maximum duration for roving orders, it would have said so. Yet neither 18 U.S.C. § 2518(11)(a), governing roving oral intercept orders, nor section 2518(11)(b), governing roving wiretap and electronic communications orders, specify any duration other than thirty days. It follows, therefore, that if an applicant can show that X, the suspect under investigation, makes a habit of choosing different locales for meetings with his coconspirators, a judge may issue a thirty-day roving oral intercept order.235

Suppose the agents have established probable cause to bug X's office, but have no direct evidence that X uses any other location to discuss his criminal schemes. May the government nonetheless seek, and a court issue, a roving oral intercept order? The answer depends on which of two interpretations of the statutory language

---

231 This was so because 18 U.S.C. § 2518(1)(b)(ii) requires an application, and section 2518(4)(b) requires an interception order, to contain a "particular description of the location where communications are to be intercepted."

232 It can take days (and, at an absolute minimum, hours) to draft the papers, submit them for review, and obtain the necessary approvals. See supra notes 181-209 and accompanying text.

233 Whether agents would have the technology needed to implement the order is, of course, a separate question, and is beyond the scope of this Article.


235 As observed earlier, supra note 233, I will not discuss the practical difficulties agents are likely to encounter in implementing such a court order.
and legislative history is correct: the "particularized showing" approach or the "or wherever clause" approach.

Under the "particularized showing" approach, an application for a "roving bug" order must make a particularized factual showing why the standard facilities-or-location specification requirement is not practical. In other words, the application would have to show that X has in the past moved from room to room in a hotel to avoid a bug, or has set up a meeting with another suspect on a beach or a field, or the like.236

Under the "or wherever clause" approach, authorities are permitted to obtain roving bug authority in every oral intercept order, so long as the application was first approved by an appropriate official.237 This view recognizes that, as every experienced investigator knows, although criminals regularly gather in more than one location to discuss or transact their crimes,238 investigators may not have discovered these other locations before submitting the original oral interception order to a judge.

To fully appreciate the uncertainty whether, with regard to roving oral intercept orders, the second, broader approach represents the intent of Congress, let us consider how the statute and legislative history treat the corresponding question with regard to wiretaps. The statute requires that an application for a roving wiretap or electronic communication intercept order make "a showing of a purpose, on the part of [the person whose communications are to be intercepted], to thwart interception by changing facilities," and issuance of such an order is permitted only if "the judge finds that such purpose has been adequately shown."239 In a discussion of this language immediately following a discussion of the oral

---

236 These examples are taken from the Senate report quoted at supra note 230. The terms "'particularized showing' approach" and "'or wherever' approach" are mine.

237 Concerning authorization, see supra notes 216-18 and accompanying text.

238 It is a common occurrence, for example, for investigators to overhear conspirators agree to meet "in Y's hotel room," or "near the amphitheatre in the park," or even "at the other guy's place, you know, the guy that your guy got the stuff from the other time." Criminals often speak so cryptically, in an effort to confuse any investigators who may be listening in, that they themselves cannot understand what they are talking about.

provision, the House and Senate Judiciary Committee Reports, in identical passages, comment:

The rule with respect to "wire communications" is *some-what similar*. As indicated in paragraph (b), the application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. A person whose telephone calls were intercepted who said that he or she was planning on moving from phone to phone or to pay phones to avoid detection also would have demonstrated that purpose.240

The italicized portions of the above passage highlight Congress' clear intent to make a particularized, factual showing of need a prerequisite to a roving wiretap. The absence of similar language discussing oral communications suggests that such a prerequisite may not have been intended for a roving oral interception.

One might argue that Congress must have intended the same standards to apply to all roving interceptions, wire and oral, and that an explicit requirement of a particularized showing of need with regard to wiretaps was intended to apply to oral intercepts as well. But the very fact that the corresponding provision with regard to roving oral interception orders, and the congressional committees' discussions of that provision, do not say anything explicit about a similar requirement, suggests that the committees did not intend to impose such a requirement on roving oral interception orders.

A reason did exist, moreover, for imposing more stringent requirements on the wiretapping interception applications. Partici-

---

pants in the legislative bargaining that produced the Electronic Communications Privacy Act of 1986 have informed me that the particularized "showing of purpose" requirement in section 2518(11)(b)(ii), and the language emphasizing that requirement in the congressional reports, were added because of concerns expressed by lobbyists for the nation's telephone companies. These individuals, who participated actively in the legislative process that resulted in ECPA, wanted statutory protection for their clients, who might suddenly be told to "wire up" large numbers of pay telephones on short notice. This concern is clearly reflected in section 2518(12), obliging investigators, if at all possible, to specify in the application and order the telephones likely to be involved, and authorizing a telephone company to move to quash a roving wiretap order that is too burdensome.241

In view of this influence, and its nonapplicability to oral intercepts, it is probable that Congress intended to permit Justice Department officials to seek and obtain roving oral intercept orders even in the absence of the kind of particularized showing of need that is required for a wiretap. It is not likely, however, that the issue will be tested in the courts in the foreseeable future. If the Justice Department's track record with the emergency provision is any indication,242 the Department will proceed very cautiously with regard to roving taps and oral intercepts.

4. Description of communications. 18 U.S.C. § 2518(1)(b)(iii) requires each Title III application to contain a "particular descrip-

241 Section 2518(12) provides:
An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subsection (11)(b) may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the government, shall decide such a motion expeditiously.


242 See supra notes 181-209 and accompanying text.
tion of the type of communications sought to be intercepted.' Section 2518(4)(c) imposes the same requirement on the interception order. Without significant exception courts have held that these requirements are satisfied by a statement including the facilities or place to be surveilled and the crimes to which such communications are expected to relate. A standard application and order must also include the identities of the individuals whose communications are to be intercepted, if known. As interpreted by the Supreme Court, this latter requirement is not an aspect of particularity, but serves only lesser purposes.

A roving intercept order, by contrast, need not specify the facilities or place. Hence, the "particularity" in the description of communications must be supplied in a different way: the identity of the individual(s) to be intercepted. Thus, the description could not be worded in terms of "communications of X and others, as yet unknown." Rather, the description would have to be expressed as "communications of X with others" or the like. Such language emphasizes that there is no authority to listen unless X is in fact a participant in the conversation.

---

243 See, e.g., the cases cited in supra note 129.
245 See supra notes 124-52 and accompanying text.
246 See supra note 148 and accompanying text.
247 It is, however, intended by Congress that even a roving intercept order specify a reasonably limited geographic area, the number of phones involved, if known, and the time within which the interception is to be accomplished. See S. REP. No. 541, 99th Cong., 2d Sess. 32, reprinted in 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3586.
248 If investigators have probable cause to bug or tap a particular location or telephone, and also have the basis for a roving intercept order, they could seek separate orders. The first would be a standard "and others, as yet unknown" order for the specific location or phone for which probable cause exists, and the second would be a roving intercept order to cover "communications of X with others" of other locations or phones. In such a case, applications for each order should include a statement that the other order is also being sought, particularly if the two orders are being submitted to different judges.

Alternatively, officials could seek a dual order. Assume that agents obtain a standard location-specific oral intercept order to bug X's office, and also obtain authority to conduct a roving oral intercept of X's conversations in other locations that relate to the crime under investigation. Such an order might authorize (1) "interception of communications of X and others, as yet unknown, which occur in X's office at Suite 12, 345 West 57th Street," that relate to the crimes under
B. Implementation of Roving Intercept Orders

Implementation of a roving intercept order differs from that involving a standard order in at least four respects: the state of investigators' knowledge about the communication facility or location to be monitored, the timing of installation of devices pursuant to the order, techniques for minimization, and the role of the telephone company.2

1. Knowledge of facilities or location. The first sentence of 18 U.S.C. § 2518(12) provides that interception of oral, wire or electronic communications pursuant to a section 2518(11) roving interception order "shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order."220 On its face, this passage seems merely to state the obvious principle that an agent cannot tap a phone, bug a location or monitor a facility until he knows which phone to tap, which place to bug, or which facility to monitor. The Senate and House Judiciary Committee discussions of section 2518(12) make clear, however, that the language has a significance greater than that. After restating the statutory language, the reports continue: "In other words, the actual interception could not begin until the suspect begins or evidences an intention to begin a conversation."221

2. Anticipatory installation of devices. Although actual interception may not begin until the suspect evidences an intent to begin a conversation, there is nothing in the statute or the House and Senate report that prohibits the installation of the equipment necessary to intercept such a conversation in advance.222 The Senate investigation, and (2) "interception of communications of X with others, wherever they occur," that relate to the crime under investigation.

249 Most electronic communications (including, for example, electronic mail and computerized transmission of data) are transmitted at least in part over telephone lines. Interception of communications transmitted and received exclusively by radio likely would not involve telephone companies.

220 The full text of section 2518(12) is set out at supra note 241.


222 The Senate Judiciary Committee Report comments: "It would be improper
Report's emphasis on the impropriety of "intercept[ing] all conversations over such phones" suggests that merely installing the taps, without intercepting conversations over the tapped phones, would not be improper. Moreover, the very purpose of the roving intercept provision supports the legality of advance installation of wiretap equipment. The provision "[is] necessary to cover circumstances under which law enforcement officials may not know, until shortly before the communication, which telephone line will be used by the person under surveillance."254

The Senate Report stresses the wisdom of including within the application and order as much information concerning likely telephones as possible because "a telephone company may not be able to respond instantaneously to an eleventh hour target line designation."255 It also explicitly encourages "law enforcement officials to continue the current practice of consulting with telephone company employees regarding the details of implementation (such as phone numbers and the specific locations of the telephones) in advance of the time any order for interception is sought,"256 a practice that reduces delays between when an interception order is issued and when it is implemented. The message seems clear enough: if the agents can predict in advance which telephones their suspect is most likely to use, they, and the telephone company, should install the necessary equipment as soon as the order is issued. 18 U.S.C. § 2518(12) merely makes it clear that before a conversation

---

253 See supra note 252.
254 S. REP. No. 541, 99th Cong., 2d Sess. 32, reprinted in 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3586. Careful study of this report reveals that section 2518(12) does not prohibit, and in fact affirmatively approves of, other techniques that enhance the usefulness of a roving wiretap or electronic communication intercept. The report does not mention roving electronic communication interception orders in its discussion of 18 U.S.C. §§ 2518(11)(b), 2518(12). However, since section 2518(11)(b) explicitly governs roving interception of electronic communications as well as roving wiretaps, however, it is reasonable to assume that discussion of the latter applies as well to the former.
255 Id. at 32, reprinted in 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3586.
256 Id. at 33, reprinted in 1986 U.S. CODE CONG. & ADMIN. NEWS 3555, 3587.
on any of the telephones can be intercepted, the burden is on the investigative agency to ascertain that the person under surveillance is about to use it.

The general question of whether roving interception orders are constitutional is deferred until later in this Article. It is worth noting here, however, that advance installation of wiretap equipment does not raise any apparent constitutional concerns. Barring extraordinary circumstances, the connections required to tap a telephone are never done inside the premises where the phone is located. They are done outside, usually at a telephone company facility. Hence, installing the necessary equipment does not constitute a physical search and seizure. Nor, if recent Supreme Court dictum may be relied upon, would this procedure constitute an electronic "search" of the telephone so long as the agents left the equipment turned off, and did not listen to or record any conversations on the tapped telephone.

It is logical to assume that section 2518(12), as explained by the Judiciary Committee Report, applies equally to oral intercepts. Indeed, in its initial comment, the Committee said as much. It is curious, however, that the rest of the Committee's discussion of

257 See infra notes 284-301 and accompanying text.
258 In United States v. Karo, 468 U.S. 705 (1984), police, acting with the consent of the seller, installed an electronic tracking device into a container of chemicals, which was thereafter sold to a person suspected of manufacturing illicit drugs. In the course of holding that the installation and subsequent sale did not constitute a Fourth Amendment search, the Court commented:

The mere transfer to Karo of a can containing an unmonitored beeper infringed no privacy interest. It conveyed no information that Karo wished to keep private, for it conveyed no information at all. To be sure, it created a potential for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. A holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on. It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.

Karo, 468 U.S. at 712. The analogy of an unmonitored wiretap to the turned-off parabolic microphone is too obvious to belabor. For an exhaustive discussion of Karo and related issues, see Fishman, supra note 53.
section 2518(12) focuses exclusively on wiretaps. Does this suggest that the provision should have a different application to oral intercepts than it does to wiretaps? There is little other support for such a distinction.

Just as agents may not, pursuant to a roving wiretap order, continuously monitor several telephones on the chance that the suspect will occasionally use them,\(^{260}\) they may not install eavesdropping devices in several locations, listen to and record everything that is said in each of them, and then later delete conversations in which the designated interceptee did not participate. To do so would clearly be contrary to a fundamental purpose of Title III, the protection of the privacy of conversations,\(^{261}\) and would probably violate the Fourth Amendment.

Similarly, the passages in the Report that make it clear that agents may install wiretaps on likely telephones before the suspect reveals his intention to use any particular phone on a specific occasion\(^{262}\) should apply equally to oral intercepts. The need to react quickly will often be just as great with regard to oral intercepts as with wiretaps. Just as a telephone company may not be able to respond to an "eleventh-hour" demand for "target-line designation," it is often impossible for investigators to install a listening device in a location at the last minute.

The very purpose of section 2518(11)(a), authorizing roving oral interception orders, is to enable investigators to react promptly and effectively when specification of the location of the target conversation is not practical.\(^{263}\) Using the example given in the congressional reports,\(^{264}\) if the agents have reason to believe that the suspect has access to several rooms in the same hotel, and he may move from room to room to avoid a bug, the agents should be allowed to implant listening devices in those rooms pursuant to section 2518(11)(a). Certainly nothing in section 2518(12) or in the House or Senate Judiciary Committees' discussions of that provision mandates to the contrary.

\(^{260}\) See supra note 252.

\(^{261}\) See supra note 8 and accompanying text.

\(^{262}\) See supra notes 252-58 and accompanying text.

\(^{263}\) See supra note 212.

There is something more than faintly Orwellian, of course, about the prospect that law enforcement officials can bug any number of hotel rooms, offices, or homes, all on the chance that a suspect might at some point during the authorized interception period choose to discuss his past, present or future crimes in one of them. Even accepting that the agents could not legally monitor these bugs until the suspect identified in the order actually goes inside one of those locations, there is perhaps no other aspect of Title III, or of any other legally authorized investigative technique, that has greater potential for abuse. Nevertheless, this is apparently what Congress has authorized in the roving intercept provision. If this was intentional, rather than inadvertent, it demonstrates considerable faith in the officials who make law enforcement policy, and those who implement that policy. Fortunately, the Justice Department’s twenty-year record in employing Title III suggests that that faith is well-deserved.265

If anticipatory installation of listening devices can be effected without physical trespass266 no significant constitutional questions are raised. The anticipatory installation of listening devices inside a private location, on the other hand, raises far more difficult questions because of the need to make physical entry, an act which itself has always been considered a search.267 Such entries, unless authorized by a valid warrant, are presumptively unlawful.268 Whether a roving intercept order may validly authorize physical

265 Except for the numerous Title III orders ruled invalid for Giordano-type violations that occurred during the tenure of John Mitchell as Attorney General, discussed at supra notes 140-41, the government’s use of Title III has been upheld in the overwhelming majority of cases in which an application, warrant or the conduct of a court-authorized interception has been challenged. Moreover, the caution with which the government has utilized the already existing emergency surveillance provision, discussed at supra notes 20, 205-08, suggests that the roving interception provisions will be utilized only very rarely.

266 An example would be the use of a parabolic microphone, see supra note 258, which is put into place but not monitored until police acquire information that the named suspect is “on location.”


268 Each of the cases cited supra note 267 so holds.
entrance into a private location that the order does not "particularly describe" in any traditional sense, is discussed subsequently.269

3. Minimization. As we have seen, 18 U.S.C. § 2518(12) provides that, when executing a roving interception order, investigators cannot begin monitoring "until the suspect begins or evidences an intention to begin a conversation."270 Continuous monitoring while waiting for the suspect to arrive at the target location is prohibited.271 The roving interception provisions are silent as to minimization practices to be followed once the suspect is known to be at that location. In the absence of explicit provisions, the most logical inference is that Congress intended the general minimization provision, 18 U.S.C. § 2518(5),272 to apply.

With regard to wiretaps, once agents have a valid reason to believe that their suspect is "on site," they should be permitted to monitor all phone calls for a brief period to determine whether the suspect named in the order is one of the conversants. If he is, they may continue to monitor the call, subject to standard minimization requirements.273 If the suspect is not a participant, they should cease monitoring, although they would be justified in spot-monitoring274 the call periodically to determine whether the suspect has become a participant. If he has, they should continue to monitor the call for as long as he is on the line.

Similar procedures should apply to minimizing a roving oral intercept. Once agents learn that their suspect is inside the target location, they should be permitted to monitor all conversations that occur within the suspect's probable range of hearing, even if the suspect does not say anything, since even a person's silence in a non-custodial interrogation setting may be revealing of guilty involvement or knowledge.275 If the "roving bug" is in a private premises and the agents cannot see whether the suspect is in the

---

269 See infra notes 302-07 and accompanying text.
270 See supra note 251.
271 See supra note 252.
272 Minimization is discussed at supra notes 150-58 and accompanying text.
273 See supra notes 150-58.
274 See supra note 152 and accompanying text.
275 See, e.g., U.S. v. Giese, 597 F.2d 1180, 1185-96 (9th Cir. 1979); U.S. v. Williams, 577 F.2d 188, 194 (2d Cir. 1978); U.S. v. Kilbourne, 559 F.2d 1263, 1265 (4th Cir. 1977); U.S. v. Gala, 544 F.2d 940, 946 (8th Cir. 1976).
room covered by the device, the only practical option is for the monitors to make a good-faith determination whether the suspect is likely to be in the room or not, and to spot monitor frequently if he apparently is not present when the surveillance commences.

Similarly, officers executing a roving electronic communication interception order should not intercept any communications over a particular facility unless they have reason to believe that their suspect is transmitting or receiving an electronic communication over that facility. When such is the case, they should minimize as with any electronic communication.276

4. Telephone company cooperation. It is difficult to effectively implement a wiretap or interception of electronic communications without cooperation of the telephone company or other communications service which services the targeted telephone or other communication facility. Accordingly, the final paragraph of 18 U.S.C. § 2518(4) provides that any Title III interception order may direct telephone companies, landlords, and the like to cooperate with the implementation of such an order.

Implementation of a roving wiretap or electronic communication interception order will often be impossible without cooperation of the telephone company that services the phones in question. The question of telephone company cooperation was the focus of considerable attention when sections 2518(11), (12) were drafted.277 This concern is reflected in the statute and in the Senate Judiciary Committee Report.278

The Senate Report specifically encourages law enforcement officials to consult with telephone company employees prior to submitting a wiretap application to obtain information they will need to implement a wiretap order once it is issued,279 and this is in fact common practice. The Senate Report also made it clear that


277 See supra note 241 and accompanying text.


the judge to whom a roving tap application is submitted should, in deciding whether to issue the order, consider whether the application and proposed order specify a reasonably limited geographic area, the number of phones and phone numbers involved, if known, and the time within which the interception is to be accomplished.250

The Senate added a second sentence to the House version of section 2518(12) which permits "[a] provider of wire or electronic communications that has received an order [for a roving wiretap to] move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion."281 The final sentence of section 2518(12) directs that "[t]he court, upon notice to the government, shall decide such a motion expeditiously."282 The failure to specify number of telephones, geographic area, and phone numbers in the application and order "may be considered evidence of unreasonableness or untimeliness by a court acting upon a telephone company motion made pursuant to [section 2518(12)]."283

C. Constitutionality of the Roving Intercept Provision

1. In general. The Fourth Amendment directs that "no warrants shall issue" which fail to "particularly describ[e] the place to be searched."284 The basic argument in favor of the constitutionality of the roving intercept provision is that the provision does not unconstitutionally waive the particularity requirement, it merely describes the "place" to be searched in a somewhat untraditional but

250 Id. at 32, reprinted in 1986 U.S. CODE CONG. & ADMN. NEWS 3555, 3581. A stated purpose for this is "so as not to render telephone company cooperation technically infeasible." Id.
282 Id. The Senate Judiciary Committee Report comments:
This provision recognizes that a telephone company may not be able to respond instantaneously to an eleventh hour target line designation. It is designed to account for the practicalities of telephone company response time, the number of phones that may be covered by the order, and the geographic area of the target lines that may be used by the person under surveillance.
283 Id. at 33, reprinted in 1986 U.S. CODE CONG. & ADMN. NEWS 3555, 3582.
284 See supra note 24 for the full text of the Fourth Amendment.
still sufficiently particular way. The description is not a specific phone or facility or location, rather any phone, facility or location X uses at a particular time. The particular description simply follows X from place to place. Agents may monitor a particular phone, location or facility, however, only if and when they reasonably believe that X is about to or is presently conversing or communicating on that particular phone, location or facility.\footnote{See supra notes 250-69 and accompanying text.}

How does this argument measure up against existing Fourth Amendment case law? There is, of course, no Supreme Court decision directly on point. Two decisions address situations that can be considered somewhat analogous, however: \textit{United States v. Steagald}\footnote{451 U.S. 204 (1981).} and \textit{United States v. Karo}.\footnote{468 U.S. 705 (1984).} Unfortunately, they point in opposite directions.

\textit{Karo} appears to support the constitutionality of the roving interception provision. There, the Court held that a warrant is usually required before the authorities may monitor the presence of an electronic tracking device inside someone’s home or other private location.\footnote{\textit{Id.} at 717. In \textit{Karo}, a beeper was hidden in a drum of chemicals. For a detailed discussion of \textit{Karo} and related issues see Fishman, supra note 53.} The Court went out of its way to state, however, that such a warrant would not have to specify in advance the place to be electronically “searched” by the device.\footnote{\textit{Karo}, 468 U.S. at 718.} It would suffice if application and warrant described the device, the object into which it is installed, and the reasons underlying the use of the device.\footnote{\textit{Id.} Congress has since incorporated this dictum into legislation as part of the Electronic Communications Privacy Act of 1986. See 18 U.S.C. § 3117 (Supp. IV 1986).} If such a warrant is constitutionally permissible in the context of electronic tracking devices, why not in the context of listening devices as well?

The argument against the \textit{Karo} analogy is simple to state and difficult to refute. First, \textit{Karo} involved a “beepered” object the location of which was the very information that was sought; in a roving interception, the location is determined before the search occurs. Second, the electronic search in \textit{Karo} is far less intrusive
than a traditional search and seizure, revealing only whether the beepered object is inside the location being monitored. The electronic "search" involved in a wiretap or eavesdrop, by contrast, is far more intrusive than a physical entry and search, by virtue of its surreptitious nature, its duration and the information it reveals. Thus, the Karo dictum, though easing the particularity requirement, provides at best an imperfect analogy to, and hence only limited support for, the roving intercept clause.

The reasoning of Steagald, moreover, supports the conclusion that the roving intercept clause is not constitutional. In Steagald, Drug Enforcement Administration agents had obtained a warrant authorizing the arrest of a man named Lyons. The agents entered and searched Steagald's home, believing Lyons was hiding there. In the course of their search, they did not find Lyons, but did find cocaine and other evidence incriminating Steagald, and they charged him with possession. The Supreme Court ruled that the entry and subsequent search of Steagald's home was unlawful. The mere fact that the agents possessed an arrest warrant for Lyons "did absolutely nothing to protect [Steagald's] privacy interest in being free from an unreasonable invasion and search of his home." Hence, from Steagald's perspective, the search "was no more reasonable ... than it would have been if conducted in the absence of any warrant." Evidence incriminating Steagald was therefore suppressed.

The analogy between Steagald and a roving intercept order is clear enough. The mere fact that officials have a court order authorizing the interception of X's telephone conversations does not protect Y's privacy interest in being free from an unreasonable invasion and search of his phone. This would be true even if the police developed probable cause to believe that X was using Y's

292 See supra note 11 and accompanying text.
294 Id. at 216.
295 Id. at 205-06. Had the police found Lyons in Steagald's home and seized evidence that incriminated Lyons, that evidence would have been suppressed only if the courts found that the seizure violated Lyons' rights. See generally W. LaFave, 3 SEARCH AND SEIZURE §§ 11.3, 11.4 (2d ed. 1987).
telephone. The Fourth Amendment requires that, barring exigent circumstances, the determination of probable cause must be made by a "detached and neutral magistrate" prior to entry.\(^\text{296}\)

Yet the *Steagald* analogy is also imperfect. Entry into a third person's home to search for someone named in an arrest warrant is much more intrusive than a properly minimized roving intercept order. When agents enter to make an arrest, objects come into plain view that are not visible to those outside. If the person sought does not immediately surrender, the intrusion intensifies as police search from room to room, and even if the arrestee promptly gives himself up, police may conduct a security sweep of the premises.\(^\text{297}\) In a roving intercept wiretap, on the other hand, no intrusion at all occurs until the police actually monitor the phone,\(^\text{298}\) and the monitoring is authorized only when the police reasonably believe that X is using or is about to use the phone. Even then, they may monitor only those conversations in which X participates, only spot-monitoring others.\(^\text{299}\) Thus, *Steagald* may be as easily distinguished from roving intercept orders as *Karo*.

In addition, there are three other arguments supporting the constitutionality of roving intercept orders. First, in at least some instances, the need to intercept conversations may arise in circumstances that may be deemed constitutionally "exigent," and the roving intercept would be constitutional under the exigent circumstances doctrine even without Title III authorization.\(^\text{300}\) Thus, the roving intercept provision, far from being unconstitutional, may be viewed as a congressional decision to impose more stringent standards on a particular class of surveillance than the Constitution would otherwise require. Second, flexibility in interpreting the Constitution should not be one-sided. If the Fourth Amendment is flexible enough to protect privacy against technological develop-


\(^{297}\) In Payton v. New York, 445 U.S. 573, 589 (1980), the Court acknowledged that law enforcement officials might sometimes need to conduct such sweeps.

\(^{298}\) See supra notes 257-58 and accompanying text.

\(^{299}\) See supra notes 270-76 and accompanying text.

\(^{300}\) See supra notes 32-91 and accompanying text for a discussion of the exigent circumstances doctrine.
ments far beyond the contemplation of the founding fathers, as it should be, then it also must be flexible enough to permit investigators to preserve the basic mandate of the amendment’s particularity requirement in novel ways. The roving intercept provision is an ingenious and carefully drawn legislative scheme that does just that. Finally, in a close case, a presumption in favor of the constitutionality of congressional legislation should tip the balance.\textsuperscript{301}

2. *Surreptitious Entry.* As noted earlier, all non-warrant authorized entries onto private premises are presumptively invalid intrusions into privacy.\textsuperscript{302} Surreptitious entry to install a listening device is even more intrusive. Yet in *Dalia v. United States,*\textsuperscript{303} the Supreme Court held that in implementing court-authorized eavesdropping at a particularly described location, law enforcement officials may surreptitiously break into and enter the location to install listening devices, even though the Title III court order did not explicitly authorize such entry.\textsuperscript{304} Although *Dalia* involved a location-specific order, much of the reasoning in the case appears to validate surreptitious entry conducted pursuant to the roving interception provision.\textsuperscript{305} Beyond *Dalia,* the arguments in favor of constitutional validity discussed previously\textsuperscript{306} are also generally applicable when surreptitious entry is necessary to carry out an oral roving intercept.\textsuperscript{307}

\textsuperscript{301} The Court has often cited this general principle. See, e.g., United States v. Watson, 423 U.S. 411, 415-16 (1976) (upholding statute authorizing postal officers to make warrantless searches).

\textsuperscript{302} See supra notes 268-69 and accompanying text.

\textsuperscript{303} 441 U.S. 238 (1979).

\textsuperscript{304} The Court held that the Fourth Amendment does not outlaw surreptitious entry per se, *id.* at 247-48, that Title III implicitly permits covert entry, since Congress must have been aware that such entry is sometimes necessary to implement an oral intercept order, *id.* at 249-54, that the Fourth Amendment does not require a Title III order to explicitly authorize such entry, *id.* at 255-58, and that while the Fourth Amendment and Title III leave it to law enforcement discretion to decide how a court order is to be executed, the reasonableness of their actions ultimately is subject to judicial review at a suppression hearing, *id.* at 258-59. For a critique of *Dalia,* see Goldsmith, supra note 137, at 112-18.

\textsuperscript{305} See the outline of the *Dalia* decision in supra note 304.

\textsuperscript{306} See supra notes 284-301 and accompanying text.

\textsuperscript{307} The counter arguments to the *Steagald* analogy at supra notes 297-99 and accompanying text, based on intrusiveness of the search, obviously do not apply to surreptitious entries.
V. OTHER WESTERN DEMOCRACIES: A COMPARISON

The challenge of balancing the needs of effective law enforcement and the protection of individual privacy is not one faced only by the United States. All democratic nations devoted to civil liberties and individual privacy face basically the same dilemma. It may prove helpful, therefore, to consider how three such nations, Canada, Israel and West Germany, regulate wiretapping and eavesdropping in general, and in particular how they regulate such surveillance in exigent circumstances. The following review of Canadian, Israeli and West German law deals exclusively with statutory regulation of wiretapping and eavesdropping for law enforcement purposes. Use of such surveillance in defense of national security raises entirely different issues, which are beyond the scope of this Article.

A. Canada

1. The statute in outline. Canada's "Interception of Communications" law is in many respects substantially similar to Title III. A court order is required to authorize the interception of all "private communications." Such orders, labeled "authorizations," may be obtained only to investigate specified serious felonies. An application for an interception order must be signed by the Solicitor General of Canada, or by the Attorney General of

308 In Great Britain, wiretapping is regulated administratively; no judicial oversight occurs. See The Interception of Communications in Great Britain, 1980, Cmd. No. 7873 (a "white paper" issued by the British government detailing the procedures followed there). Because of the absence of judicial participation, an analysis of British procedures is not included here. For an overview, see Note, Secret Surveillance and the European Convention on Human Rights, 33 Stan. L. Rev. 1113, 1122-29 (1981).


310 Communications are protected only if the conversants have a reasonable expectation that what they say is not being intercepted. Tremear's Crim. Code § 178.1 (1988) (definition of "private communication"). This provision closely parallels the Title III definition of "oral communication," 18 U.S.C. § 2510(2) (Supp. IV 1986). A person is not protected from the interception of his communications if another party to a communication consents. Tremear's Crim. Code §§ 178.11(2)(a), (b), (3) (1988). This provision is substantially identical to 18 U.S.C. §§ 2511(2)(c), (d) (Supp. IV 1986).

the province in which the application is made, or by an agent specially designated in writing by one of those officials.\textsuperscript{312}

The application must specify the facts relied upon to justify the issuance of an interception order,\textsuperscript{313} the type of private communications sought to be intercepted,\textsuperscript{314} the "names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable and probable grounds to believe may assist the investigation of the offense,"\textsuperscript{315} and a statement as to all previous applications made in connection with any targets named in the current application.\textsuperscript{316} If a prior application had been withdrawn or rejected, this information must also be included, together with the name of the judge to whom the prior application had been made.\textsuperscript{317} Further, the application must state whether other investigative procedures have been tried and have failed, or why they are unlikely to succeed if tried.\textsuperscript{318}

A judge may issue such an order only if he or she is satisfied that the application makes adequate factual showings.\textsuperscript{319} A special showing of need is required to authorize interception of conversations between a solicitor and client, and the judge is empowered to insert into the order special provisions protecting privileged communications.\textsuperscript{320} The order must specify the offense involved, the type of communication to be intercepted, the targeted individuals and locations, if known, and must generally describe how the interceptions are to be achieved.\textsuperscript{321} In issuing the authorization, the judge may impose conditions he or she "considers advisable in the

\textsuperscript{312} \textit{Id.} § 178.12(1) (which corresponds closely to 18 U.S.C. §§ 2516(1),(2) (1982 & Supp. IV 1986)).

\textsuperscript{313} \textit{Id.} § 178.12(1)(c).

\textsuperscript{314} \textit{Id.} § 178.12(1)(d) (compare 18 U.S.C. § 2518(1)(b)(iii) (Supp. IV 1986)).

\textsuperscript{315} \textit{Id.} § 178.12(1)(e) (apparently the equivalent of the Title III probable cause requirement).

\textsuperscript{316} \textit{Id.} § 178.12(1)(e.1) (corresponding to 18 U.S.C. § 2518(1)(e) (Supp. IV 1986)).

\textsuperscript{317} \textit{Id.}

\textsuperscript{318} \textit{Id.} § 178.12(1)(g) (substantially identical to 18 U.S.C. § 2518(1)(c) (1982)).

\textsuperscript{319} \textit{Id.} § 178.13(1) (substantially identical to 18 U.S.C. § 2518(3) (1982 & Supp. IV 1986)).

\textsuperscript{320} \textit{Id.} §§ 178.13(1.1), (1.2). Title III has no provisions corresponding to these.

\textsuperscript{321} \textit{Id.} §§ 178.13(2)(a), (b), (c) (18 U.S.C. § 2518(4) (1982 & Supp. IV 1986) is similar in most respects).
An order may authorize interceptions for up to sixty days. Renewals are permitted, but only upon an additional factual showing of continued need and of progress made to date.

The Canadian statute contains an exclusionary rule similar to that included in Title III. Privileged communications are protected from improper disclosure. Within ninety days of the completion of interception, the targets of the surveillance must be notified that their communications were intercepted, except that postponements of notice are permitted upon a showing of good cause. Premature or unauthorized disclosure may be punished by up to two years' imprisonment. Before an intercepted communication may be offered in evidence, adequate notice of the prosecutor's intent to do so must be provided.

The Canadian statute thus reflects the same concerns, and employs many of the same mechanisms, as Title III. There are, however, significant differences. Canada's law contains no minimization provision, for example, and it is more difficult for a Canadian

322 Id. § 178.13(2)(d) (corresponding to 18 U.S.C. § 2518(3) (1982 & Supp. IV 1986)).
323 Id. § 178.13(2)(e). The corresponding period in Title III is 30 days. 18 U.S.C. § 2518(5) (Supp. IV 1986). In Berger v. New York, 388 U.S. 41, 59 (1967), the Supreme Court held that 60 days was too lengthy a period to permit surveillance based upon a single showing of probable cause.
325 Id. § 178.16(1). The statute limits, however, the application and impact of the "fruit of the poisonous tree doctrine," id. §§ 178.16(1), (2), and permits a judge to admit into evidence communications intercepted pursuant to a statutorily imperfect order if the imperfection is "only . . . a defect of form or an irregularity in procedure," rather than a "substantive defect or irregularity." Id. § 178.16(3). This provision corresponds to the judicially-created rule in the United States that violations of aspects of Title III that were intended to play a substantial role in limiting the use of electronic surveillance require suppression of evidence, but violation of less significant provisions does not require suppression of evidence. United States v. Giordano, 416 U.S. 505, 527 (1974); United States v. Chavez, 416 U.S. 562, 571-72, 579-80 (1974).
327 Id. § 178.23 (corresponding to 18 U.S.C § 2518(8)(d).
328 Id. § 178.2(1) (corresponding to 18 U.S.C. § 2511(1) (1982 & Supp. IV 1986), which imposes up to five years' imprisonment).
329 Id. §§ 178.16(4), 178.17 (corresponding to 18 U.S.C. § 2518(9) (Supp. IV 1986)).
defendant to challenge the adequacy of a court order and the application submitted in support thereof. Two additional distinctions are particularly pertinent to the question of exigent surveillance. First, Canada’s statute has a “basket clause” that is similar to, but broader than, the Title III roving intercept provision. Second, Canada has an emergency surveillance provision that is different in some respects.

2. The locational “basket clause.” The standard Title III application and order must contain “a particular description of the nature and location of the facilities from which or the place where communication is to be intercepted.” Canada’s statute, by contrast, requires an application to provide only “a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted . . . .” Similarly, the order need only “generally describe the place at which private communications may be intercepted, if a general description of that place can be given.”

Relying upon this language, Canadian officials frequently seek and receive judicial authorization to intercept communications of specified individuals at specified locations, and, in addition, authorization to intercept the communications of those individuals at any other location within the jurisdiction of the court that are “resorted to or used by” the specified individuals. Such a provision in the order, which Canadian courts bluntly refer to as a “basket clause,” has been upheld by every court that has considered the issue.


331 18 U.S.C. § 2518(1)(b)(ii) (Supp. IV 1986) (emphasis added). See also id. § 2518(4)(b), which requires an interception order to “specify . . . the nature and location of” the phone to be tapped or the place to be bugged.


333 Id. § 178.13(1.2)(c) (emphasis added).


The parallels between the Canadian "basket clause" and the new roving interception provision of Title III are not completely coincidental. Indeed, the Canadian provision probably was at least in part the inspiration for the 1986 amendment to Title III. There are only two significant differences. First, the basket clause is automatically included in a Canadian court order whenever the prosecutor seeks it, while an application for a roving intercept must be specially approved and specially justified. Second, Canadian officials use the basket clause provision on a regular basis, while American officials in all likelihood will not regularly use roving intercepts.

3. The emergency surveillance provision. If an investigator believes that a compelling need exists to intercept communications before an application for authorization can be processed that complies with statutory procedures, and if he is authorized in writing by the Solicitor General of Canada or by the Attorney General of a province, the investigator may apply to a specially designated judge for written authority to intercept communications for up to thirty-six hours. Communications intercepted pursuant to this

113, 119-20, 124-25 (Vancouver County Ct., B.C., 1979); Regina v. Vrany, 46 C.C.C.2d 14, 19-20, 23 (Ont. App. 1979); Regina v. Niles, 40 C.C.C.2d 512, 514 (Ont. App. 1978). But see Regina v. Blacquiere, 57 C.C.C.2d 330, 337-38 (P.E.I. Sup. Ct. 1980) (holding that either the person or place must be known). The courts are divided, however, as to whether an intercepted communication itself suffices to show that the targeted individuals "resorted to" a location other than that specified in the authorization, or whether it is necessary to show that the authorities had evidence independent of and preceding the interception justifying a belief that the suspect "resorted to" a location not specified in the order. Of the cases cited in this note, Newall and Biasi hold that the interception itself suffices; Vrany suggests likewise. Lyons and Niles, by contrast, hold that the prosecution cannot use the communication itself to prove that the targets "resorted to" the telephone in question, because evidence that the targets resorted to that telephone is necessary to show that the police were lawfully tapping that previously undesignated telephone in the first place.

Officials in the Justice Department and on the staff of the President's Commission on Organized Crime, for which I acted as a consultant until the Commission was "defunded" out of existence in 1986, were well aware of the Canadian "basket clause" in 1985-1986. It was during this period that various legislative proposals were taking shape that now make up the Electronic Communications Privacy Act of 1986.

See supra notes 215-48 and accompanying text.

See supra notes 18-20 and accompanying text.

procedure are admissible only if the judge subsequently certifies that, had an application been submitted to him under the regular procedures, he would have granted the application.\textsuperscript{340}

Viewed in isolation, this provision seems more demanding in several respects than 18 U.S.C. § 2518(7), but in context it is not. Both statutes require approval by a high prosecutorial official, but the Canadian statute also requires judicial approval and permits emergency surveillance for a shorter period of time.\textsuperscript{341} The Canadian provision apparently does not, however, require the submission of a statutorily satisfactory retroactive application, as does Title III.\textsuperscript{342} Further, Canada's "basket clause" provision greatly reduces the need to invoke the emergency surveillance provision. The latter seems to apply only where an entirely new investigation is to be commenced that does not involve individuals who are the targets of an existing interception authorization. Thus, on the whole the Canadian statutory scheme gives law enforcement personnel a latitude in intercepting communications that is at least as broad as that of Title III.

\textbf{B. Israel}

Israel's statute\textsuperscript{343} covers both eavesdropping and wiretapping.\textsuperscript{344} Anyone who secretly monitors a conversation without lawful authority may be punished by up to three years imprisonment.\textsuperscript{345} Such monitoring for law enforcement purposes\textsuperscript{346} is lawful only if a court

\textsuperscript{340} \textit{Id.} § 178.15(3).

\textsuperscript{341} The Canadian statute permits emergency surveillance for 36 hours, \textit{id.} § 178.15(2), while Title III allows 48 hours, 18 U.S.C. § 2518(7) (Supp. IV 1986).


\textsuperscript{343} 33 L.S.I. 141 (5739-1979) (5739 is the year in the Hebrew calendar; 1979, the year in the secular calendar). All citations in the following analysis refer to an unofficial translation of the Israeli statute which appears at Note, \textit{Digest: Recent Legislation and Cases}, 15 \textit{Israel L. Rev.} 131, 144-53 (1980).

\textsuperscript{344} 33 L.S.I. 141 § (5739-1979) 1 defines "listening" as listening to the conversation of another by means of a device, "eavesdropping" as listening without the consent of any of the parties to the conversation, and "conversation" as conversation by word of mouth or other means of communication.

\textsuperscript{345} \textit{Id.} § 2(a).

\textsuperscript{346} The statute also regulates monitoring for purposes of state security. \textit{Id.} § 4. This provision is distinct from those regulating law enforcement monitoring, and is therefore beyond the scope of this study.
order, or "permit", is issued by the President of a District Court.\(347\) The application for such an order must be submitted in writing by a police officer of the rank of nitzav mishne (approximately colonel) or higher, who has been authorized to do so by the Inspector-General of Police.\(348\)

The judge may issue a permit "if he is satisfied that it is necessary to do so to prevent offenses or detect offenders."\(349\) The permit "shall indicate the identity of the person whose conversations may be listened to, and the place and type of such conversations, if these data are known in advance; it shall also specify the permitted modes of listening."\(350\) Such a permit is valid for no more than three weeks.\(351\)

The statute prohibits the secret monitoring of privileged communications.\(352\) It also contains an explicit exclusionary rule,\(353\) which is noteworthy in the Israeli context because the Israeli legislature (Knesset) and courts have rejected the concept of an exclusionary rule generally.\(354\) Further, conversations lawfully recorded pursuant to the statute are admissible only "as evidence in a criminal proceeding not arising out of a private complaint."\(355\)

A comparison of Israel's statute to Title III thus reveals significant similarities. The decision to seek a court permit must be made by a highly placed government official. Monitoring must be of limited duration. It may be used only to investigate criminal offenses. Conversations intercepted in violation of the statute are not admissible in evidence.

\(347\) Id. § 6(a). Israel is divided into six administrative districts. Its trial court system is two-tiered, consisting of magistrate's court and district court, the latter being the higher of the two.

\(348\) Id. §§ 1, 6(a) (5739-1979). Although the Inspector-General of Police may authorize an application for a monitoring permit on his own authority, he is required to report monthly to the Minister of the Interior concerning the permits issued, and the terms of those permits. The Minister of the Interior, in turn, is required to transmit a copy of these reports every three months to the Minister of Justice. Id. § 6(f).

\(349\) Id. § 6(a).

\(350\) Id. § 6(d) (emphasis added).

\(351\) Id. § 6(e).

\(352\) 33 L.S.I. 141 § 9 (5739-1979).

\(353\) Id. § 13(a).


\(355\) 33 L.S.I. 141 § 13(c) (5739-1979).
There are, however, significant differences. Use of wiretapping and eavesdropping is not limited to specified crimes. The statute does not specify the factual showing required to satisfy the judge that the permit "is necessary ... to prevent offenses or detect offenders." It contains no minimization provision. Further, like Canada's statute but unlike Title III, there is no rigid requirement that the application or permit specify the locations or facilities to be tapped or bugged. Such information is to be included only if it is known at the time of the application.

Israel's statute contains an emergency surveillance provision which, like 18 U.S.C. § 2518(7), allows such surveillance without prior judicial approval. The permit for such surveillance may be issued by the Inspector General of Police, if that official is satisfied that the surveillance "must be carried out without delay in order to prevent, or detect the perpetrators of, a felony" before a judicial permit can be obtained. This permit must be in writing and must contain the same information a judicially issued permit would contain. It is valid for a maximum of forty-eight hours. Upon issuing such a permit, the Inspector General must "forthwith notify the Minister of the Interior to such effect in writing, and the Minister of the Interior may cancel the permit." Like Title III, the Israeli statute provides that communications intercepted pursuant to emergency surveillance are admissible in a subsequent trial only if retroactive approval of the permit is obtained from the president of a district court.

---

356 In assessing these differences, it is important to remember that Israel's government is more centralized than that of the United States or Canada, that its boundaries include only 8,302 square miles (excluding the West Bank and Gaza Strip), and that its estimated population in 1985 was 4.23 million, Euromonitor Publications Limited, International Marketing Data and Statistics 1987/88 4 (12th ed. 1987).
357 See supra note 349 and accompanying text.
358 33 L.S.I. 141 § 6(a) (5739-1979).
359 See supra note 350 and accompanying text.
360 33 L.S.I. 141 § 6(a) (5739-1979).
361 Id. § 7(a).
362 See supra note 350.
363 33 L.S.I. 141 § 7(a) (5739-1979).
364 Id. § 7(b). The Minister of the Interior must transmit copies of the notification to the Minister of Justice every three months. Id.
365 Id. § 7(c).
C. West Germany

Wiretapping for law enforcement purposes in West Germany is regulated by sections 100a-101 of the German Criminal Procedure Code (Strafprozessordnung). Such wiretapping is lawful only if conducted pursuant to court order, which a judge may issue only if an application relates facts which "justify the suspicion that someone . . . committed" certain serious crimes. The order may be obtained either to investigate the crime or to locate a suspect, so long as "establishing the facts or establishing the whereabouts of the accused in any other manner would be futile or rendered considerably more difficult."

The statute is silent as to which officials may apply for a wiretap order, although it provides that, upon receipt of such an order, the German Postal Service "shall make it possible for the judge, the public prosecutor, and their assistant civil servants of the police forces" to conduct the wiretap by providing the necessary technical assistance and facilities. Thus, the statute apparently contemplates prosecutorial direction and control over the process, and this apparently is how things have worked out in practice.

The wiretap order must be in writing, and must "contain the name and address of the person against whom it is directed," as

---

366 StPO §§ 100a-101 (1968). The analysis that follows is based upon a translation of the statute provided to me by the President's Commission on Organized Crime. There is apparently no regulation of eavesdropping (bugging). The same legislation that enacted StPO §§ 100a-101 also regulates wiretapping for national security purposes. The latter provisions are entirely separate from those relating to law enforcement, however, and are beyond the scope of this study. For a more detailed analysis of the West German statute and its use, see Carr, Wiretapping in West Germany, 29 AM. J. COMP. L. 607 (1981).

367 StPO §§ 100a-no.1(a)-(d) (1968).

368 Id. § 100a.

369 Id. The provision therefore appears akin to 18 U.S.C. §§ 2518(1)(c),(3)(c) (1982), which require a Title III application to demonstrate that ordinary investigatory procedures have been tried and failed, or would be unlikely to succeed if tried, or that ordinary procedures would be too dangerous.

370 StPO § 100b(III) (1968).

371 Professor Carr reports that the West German federal prosecutor's office follows a practice of centralized evaluation and review of applications before they are submitted to a judge. Carr, supra note 366, at 619-20. There is apparently little centralization with regard to applications submitted by West German state prosecutors. Id. at 620.

372 StPO § 100b(II) (1968).
well as the "type, extent, and duration of the measures" that are authorized. Such an order may be directed not only against someone suspected of the crime being investigated, but also against "persons who, on the basis of certain facts, are suspected of accepting information that comes from the suspect, or of passing it on, or of having the accused use their [telephone or teletype] line." The telephone or teletype lines of such "contact persons" may be tapped even if they are innocent associates of the target and are not themselves suspected of complicity. It is unclear whether the court order must name the specific "contact persons" whose lines may be tapped, or whether an order can grant general authorization to tap the lines of "contact persons" as investigators identify them. If the latter, the West German "contact person" provision is even broader and more permissive in scope than Canada's "basket clause" provision.

Like Title III, West Germany's statute requires that at least those who were named in the court order must eventually receive notice of the fact that their lines have been tapped. The wiretap order may have a maximum duration of three months, and may be renewed provided the requisite conditions still exist.

Unlike Title III, the order is not required to contain a "particular description of the type of communication sought to be intercepted." The West German statute also contains nothing akin to the Title III minimization provision. Nor does it contain an exclusionary rule for the fruits of wiretapping conducted in violation of the statute, although at least one commentator has theorized that suppression might result in at least some circumstances.

Like each of the other statutes examined, West Germany's wiretapping law contains an emergency surveillance provision. "In the

---

373 Id.
374 Professor Carr reports that a wiretap order cannot be issued unless a formal investigative proceeding directed by a prosecutor and supervised by a judge, roughly similar to a grand jury proceeding, has been commenced. Carr, supra note 366, at 622.
375 SrPO § 100a (final clause) (1968).
376 Carr, supra note 366, at 625.
377 See supra notes 331-35 and accompanying text.
378 SrPO § 101(I) (1968).
379 Id. § 100b(II).
381 See Carr, supra note 366, at 639-43.
case of apprehended danger . . . the public prosecutor may issue” an interception order. An order issued by a public prosecutor shall be inoperative unless it is confirmed by a judge within three days."

D. Comparison

It is clear that Title III, even with the roving intercept provision, is by far the most restrictive and demanding of the statutes examined. This should be cause for neither surprise nor dismay. More than any other society, we cherish individual dignity, liberty and privacy, particularly as against state action. No dramatic conclusions are offered as a result of this brief survey. It was offered to establish a context in which Title III and the emergency and roving intercept provisions can be assessed.

VI. Evaluation and Conclusion

When Congress enacted Title III, it established an elaborate set of procedures that must be followed before law enforcement officials are permitted to wiretap or eavesdrop. The statute was designed to strike a balance between the need to combat crime, and the protection of individual privacy. Overall, the legislation has achieved its purpose.

At times, however, situations arise in which the elaborate procedures necessary to obtain a court order cannot be completed in time for investigators to act effectively. Congress has addressed this need on three separate occasions. Title III, as enacted in 1968, included a provision crafted to permit a prompt response to emergency situations involving “conspiratorial activities characteristic of organized crime,” while preserving the essential protections of pre-interception review by an authoritative law enforcement official and timely judicial review. In 1984, Congress amended the provision to explicitly permit its use in life-threatening situations. In 1986,
Congress added 18 U.S.C. § 2518(11), the “roving intercept” provision. When its special requirements are satisfied, the provision permits investigators to obtain a court order authorizing them, in the case of a wiretap, to intercept a specified person’s telephone conversations over any phone he happens to use, or, in the case of a bug, to intercept the specified person’s oral conversations in any location where those conversations occur.

A. Evaluation

Do these provisions afford investigators with sufficient flexibility? Do they adequately safeguard individual privacy? What alternatives are worth considering?

1. The emergency surveillance provision. The emergency surveillance provision essentially provides that when a situation exists that involves “immediate danger of death or serious physical injury to any person,” or “conspiratorial activities characteristic of organized crime,” certain top Justice Department officials may authorize an investigator to intercept communications without a court order. An application for a retroactive order of approval must be submitted to a judge within forty-eight hours of the commencement of interception.

This provision has been used only in life-threatening situations, and never in a more traditionally investigative, evidence-gathering context. There are several reasons. First, section 2518(7) is based on an exigent circumstances doctrine that even now, two decades after the enactment of Title III, provides only vague guidelines as to when such surveillance would be constitutional. Second, the

---

387 ECPA, supra note 17.
389 18 U.S.C. § 2518(7) (Supp. IV 1986). For the full text of this section, see supra note 161.
390 Id.
391 See supra note 172.
392 See supra notes 32-59 and accompanying text.
provision itself is so ambiguous that it is difficult for even the
most conscientious investigators, attorneys and judges to know when
emergency surveillance would be lawful.\textsuperscript{393} Third, the Justice De-
partment has an institutional bias against approving the interception
of communications until the factual and legal justification has been
reduced to writing.\textsuperscript{394} Moreover, the attorneys with primary respon-
sibility to evaluate Title III applications insist that when circum-
stances are truly exigent, they can process an application within
hours, thereby largely eliminating the need to conduct interceptions
prior to obtaining judicial authorization.\textsuperscript{395}

There is no objective way to evaluate this assertion, or the re-
lated claim that true "emergencies" (except in the life-threatening
context) simply do not occur.\textsuperscript{396} I can only offer my own conced-
edly subjective\textsuperscript{397} impression that, when it comes to using Title III,
federal policy resembles traditional Russian military strategy: offen-
sive action is taken only after ponderous planning, preparation,
and review up through the hierarchy. Hasty mistakes are avoided,
but opportunities to seize the initiative and act quickly are forfeited
as a result. Perhaps this is as it should be, but perhaps a better
balance could be struck.

Remedial legislation could clarify some of the uncertainties that
exist with the emergency provision. The simplest alternative would

\textsuperscript{393} See \textit{supra} notes 172-75 and accompanying text.
\textsuperscript{394} See \textit{supra} notes 205-09 and accompanying text.
\textsuperscript{395} See \textit{supra} note 208 and accompanying text.
\textsuperscript{396} See \textit{supra} note 209 and accompanying text.
\textsuperscript{397} During 1969-77, while serving as an Assistant District Attorney in the New
York County District Attorney’s Office and New York City’s Special Narcotics
Prosecutor’s Office, I personally drafted and supervised the execution of some 35
wiretapping and eavesdropping warrants issued pursuant to New York’s statute,
\textit{N.Y. Crim. Proc. Law} §§ 700.05-.70 (McKinney 1984), and oversaw the drafting
and execution of several dozen others handled by other prosecutors in those
offices. In roughly half of those cases, the officials who sought my assistance
were federal agents. They preferred to work with me, and other state prosecutors,
rather than go to the United States Attorney’s Office, because we were able to
obtain a court order in less than half the time that it took federal prosecutors.
No order obtained under my direct or indirect supervision was ever successfully
challenged. On only one occasion was evidence derived from such an order sup-
pressed.

The New York statute contained no emergency surveillance provision. I can
recall at least half a dozen occasions when I would have sought authority for
such surveillance had it been legally available.
be to modify the "organized crime" language of section 2518(7)(a)(iii), perhaps by eliminating the "organized crime" requirement altogether, to afford the Attorney General with broader discretion in deciding whether to invoke it. To my knowledge, however, the Justice Department has never sought such a change. Given the Justice Department's historic reluctance to use the emergency provision, it is unlikely that such an amendment would result in a greater willingness to invoke it.

2. Decentralization of the application and authorization process. A second alternative, involving a somewhat greater revision in Title III procedures, is to permit the Attorney General to decentralize the application authorization process somewhat. Currently, before a government investigator may apply to a judge for an interception order, he or she must be authorized to do so by the Attorney General, Deputy Attorney General, Associate Attorney General, or an Assistant Attorney General specially designated by the Attorney General. In 1976, the National Wiretap Commission recommended that Congress amend this provision to permit the Attorney General to specially designate United States Attorneys and Federal Strike Force Attorneys as authorizing officials. In essence, such

---

398 I concede the irony of suggesting that a statute can be made a more effective weapon against organized crime by eliminating the reference to organized crime.

399 If such an amendment were enacted, 18 U.S.C. § 2518(7)(a)(iii) might read "other criminal conduct that is particularly serious in nature and scope," rather than "conspirational activities characteristic of organized crime." See supra note 161 for the full text of section 2518(7).

400 The Department did, by contrast, actively seek an immediate danger clause, see supra note 168, and in 1986 sought passage of the roving interception clause, see supra note 336.


402 NWC REPORT, supra note 6, at 7, 10 (1976). At the time, the application review process in Washington apparently took somewhat longer than it does now: the Commission reported that "most reviews take ten to fifteen days in Washington," id. at 58-59, although elsewhere in the Report it observed that "[t]he procedure now usually takes three to five days in Washington," id. at 7. The Report offered no explanation for the apparent conflict in its statistics. At the time, 18 U.S.C. § 2516(1) permitted only the Attorney General and specially designated assistant attorneys general to authorize applications. The addition of the Deputy Attorney General, Associate Attorney General, and specially designated acting Assistant Attorneys General and Deputy Assistant Attorneys General in the Criminal Division to the list of officials empowered to authorize applications
an amendment would allow, but not require, the Attorney General to empower specially designated United States and Strike Force Attorneys to submit a Title III application directly to a federal judge without first submitting the application to Washington for approval.

Such an amendment would constitute a far more substantial change to Title III than would occur if the emergency provision itself is amended. Yet there is considerable logic to this suggestion, particularly if one assumes that the Attorney General would specially designate only those United States and Strike Force Attorneys who are experienced in applying Title III and are knowledgeable about Justice Department policies governing wiretapping and eavesdropping. If the investigative agency also empowered its special agent in charge of the agency field office to approve the agency’s participation in the investigation, without requiring referral to the agency’s headquarters in Washington, such a measure would reduce the application review process by about a week.

There are valid arguments against decentralization. Decentralization of the authority to authorize applications might result in deviations from overall Department policy regarding when and how Title III should be used. Eliminating Justice Department review of some Title III applications might increase the risk that a statutorily inadequate application will be submitted to, and approved by, a probably speeds the application process somewhat. According to knowledgeable Justice Department spokesmen, however, the authorizing official who reviews the application, usually the Assistant Attorney General of the Criminal Division, is able to do so within a day or so, certainly not an unreasonable amount of time. The review process takes as long as it does because of the complexity of the matter being reviewed, not because of a logjam when the application reaches the authorizing official.

Congress restricted the list of officials who could authorize an application for two main reasons: it sought to assure that policies governing Title III would be determined centrally, and that the decision to employ the statute in any given case would be made by an official who was “subject to the political process.” S. REP. No. 1097, 90th Cong., 2d Sess. 97, reprinted in 1968 U.S. CODE CONO. & ADMIN. NEWS 2112, 2185. Because United States Attorneys, like the Attorney General and the Deputy, Associate, and Assistant Attorneys General, are “subject to the political process,” the amendment to Title III suggested by the National Wiretap Commission would not undermine Congress’ second reason for restricting the list of authorizing officials.

See supra text following note 193.
judge, resulting in wasted time and energy, unlawful invasion of privacy, and perhaps civil litigation.\textsuperscript{405} Even so, selective decentralization would add considerable flexibility without seriously jeopardizing the balance that Congress sought and achieved. The Justice Department, however, opposes decentralization, and until its attitude changes, it is doubtful that Congress will enact the necessary legislation.

3. The roving intercept provision. The roving intercept provision\textsuperscript{406} provides that, if authorized by someone in the top echelon of the Justice Department, a federal law enforcement official may seek a court order, targeted against a specified individual, that authorizes investigators to tap or bug all of that person’s conversations, over any phone or at any location. The provision is consistent with the overall structure of Title III and the balance that statute creates between efficient law enforcement and respect for privacy. It preserves the basic rule that there should be no interception of communications without a court order. It is also consistent with the Justice Department’s insistence that a properly drafted, written application is an absolute prerequisite for Department approval of the use of Title III.\textsuperscript{407}

The roving intercept provision appears to cut through many of the difficulties that flow from centralization of the application process and from the Justice Department’s reluctance to invoke the emergency provision. It permits prompt, decentralized response to day-to-day developments: prompt, because the statute does not require a new court order before investigators may electronically

\textsuperscript{405} 18 U.S.C. § 2520 (Supp. IV 1986) provides that “any person whose wire, oral or electronic communication is intercepted . . . in violation of this chapter” may bring a civil action against anyone involved in the violation. 18 U.S.C. § 2518(7) (Supp. IV 1986), the emergency surveillance provision, provides that should a judge refuse to issue an after-the-fact order approving the surveillance, “the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter.” Although a good-faith belief that the surveillance was lawful would constitute a defense to a civil action, 18 U.S.C. § 2520(d) (Supp. IV 1986), being required to establish good faith would likely prove expensive, time-consuming and awkward, and could embarrass or endanger those who provided investigators with the information that had prompted them to conduct the surveillance in the first place.


\textsuperscript{407} See supra notes 205-07 and accompanying text. The only exception is in life-threatening situations.
“follow” a suspect to a new phone or location; decentralized, because the statute requires Justice Department approval of the original application, but does not require the field supervisors to obtain subsequent approval of Department officials in Washington before “roving” to a new phone, facility or location.

Although there are areas of uncertainty at the margins,\textsuperscript{408} the roving intercept provision is basically straightforward. Unlike the “organized crime” clause of the emergency surveillance provision, the roving intercept provision is not flawed by a vague, ill-defined term at its very core. The provision takes an inventive approach to the Fourth Amendment particularity requirement, thereby raising some apprehension about the provision’s constitutionality.\textsuperscript{409} These doubts will in all likelihood be resolved in the provision’s favor, but only if the provision is used by the Justice Department and tested in the courts. Justice Department officials were aware of the constitutional issue when they negotiated with Congress for the inclusion of the provision in the Electronic Communications Privacy Act.\textsuperscript{410} It would be unfortunate indeed if an excess of caution prevents the Department from the judicious use of the provision.

B. Conclusion

Crime, particularly organized crime, poses a significant threat to the health, safety, and economic well-being of the nation and its citizens. Electronic surveillance is an important weapon in the arsenal against organized crime, and the Justice Department has conducted such surveillance pursuant to Title III effectively and with admirable regard for individual privacy. Developments in communications technology, however, make it easier than ever for disciplined, sophisticated criminals to maintain contact with one another while staying several steps ahead of investigators obliged to adhere to the standard Title III application process.

Although since its enactment Title III has contained a provision intended to permit investigators to respond to exigent circumstances, it has, for a variety of reasons, gone virtually unused. The government’s response to emergencies and fast-breaking develop-

\textsuperscript{408} See supra notes 226-42 and accompanying text.
\textsuperscript{409} See supra notes 284-307 and accompanying text.
\textsuperscript{410} See supra note 336 and accompanying text.
ments has also been slowed by the statutory requirement that a top Justice Department official authorize all Title III applications.

The roving intercept provision, added in 1986, constitutes a novel and ingenious attempt to enhance the speed and flexibility with which investigators can respond to fast-breaking developments. At the same time, it retains the basic safeguards that prevent unnecessary intrusions into individual privacy. While the roving intercept provision does not solve all potential problems, it can be a significant tool for law enforcement—if the Justice Department permits its investigators and prosecutors to use it.