Cornell Law Review

Volume 61
Issue 1 *November 1975*

Article 3

Post-Authorization Problems in the Use of Wiretaps Minimization Amendment Sealing and Inventories

Andrew M. Low

POST-AUTHORIZATION PROBLEMS IN THE USE OF WIRETAPS: MINIMIZATION, AMENDMENT, SEALING, AND INVENTORIES

One morning in 1969, a New Jersey detective installed a tape recorder and a set of earphones in a room overlooking a bar and liquor store. Pursuant to a court order, he was using a wiretap to overhear and record all the telephone calls made between the hours of ten a.m. and three p.m. from and to a public pay telephone in the store. The purpose of the wiretap was to catch a man named Dye making telephone calls that would provide evidence of violations of New Jersey gambling laws. Because the detective could not see the telephone from where he sat, he did not know who was making the call, so he recorded every conversation between ten and three and later rerecorded the incriminating conversations onto a second tape. Out of a total of 105 hours of recordings, two and one-half hours were incriminating and were rerecorded; the rest of the recordings were apparently irrelevant, most probably consisting of conversations of bar patrons. At Dye's trial the prosecution introduced some of the incriminating recordings in evidence, and the defense objected strenuously.[1]

The basis for the defense objection was the much-litigated and little-analyzed constitutional and statutory requirement that the agents manning a wiretap[2] must strive to minimize interception of conversations that fall outside the scope of their wiretap order. Because agents can never know exactly what they are about to hear, even if they make conscientious efforts to edit out irrelevancies—unlike the New Jersey detective—they will always intercept some conversations outside the strict scope of their order. These interceptions have often provided ammunition for defense efforts to procure suppression based on what has become known as the minimization[3] ground—the first of four wiretap problems to be analyzed in this Comment.

Since wiretapping constitutes a search and seizure, law

[1] State v. Dye, 60 N.J. 518, 291 A.2d 825, *cert. denied,* 409 U.S. 1090 (1972).

[2] The material in this Comment applies equally to wiretapping—the interception of wire communications using a listening device attached to the communication facility—and to bugging—the interception of oral communications through the use of a microphone. The term "wiretapping" will be used throughout, however, as a simple shorthand to refer to both types of eavesdropping.

[3] The term "minimization" refers to the process of limiting interception of conversations to those described in the search warrant, or, as it is commonly called in the wiretap context, the eavesdropping order. If the monitoring agent fails to minimize, he produces "overage," which is the nonpertinent portion of the intercepted conversations.

enforcement authorities must show probable cause and obtain the equivalent of a search warrant, and the operation of the wiretap itself is subject to the fourth amendment.[4] The duty of minimization arises from the particularity and reasonableness requirements of the fourth amendment, as well as from federal and state statutes.

The defense in *State v. Dye*[5] argued that the detective monitoring the wiretap had failed to minimize interception of conversations outside the scope of his warrant.[6] They claimed that the detective's failure to turn off his tape recorder and remove his earphones, even when he knew he was overhearing innocent patrons of the bar, violated both the fourth amendment and the New Jersey statute.[7] The New Jersey Supreme Court did not agree, and held that the policeman correctly listened to and recorded all the calls so long as he made an effort to limit the hours of the day during which he operated the tap.

This decision is at odds with nearly all the federal cases and illustrates the extent to which confusion and inconsistency beset the minimization case law. Although the fourth amendment and the federal wiretap authorization statutes—Title III of the Omnibus Crime Control and Safe Streets Act of 1968[8]—establish the basic minimization standards in all United States courts,[9] the resulting

[4] U.S. CONST. amend. IV provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[5] 60 N.J. 518, 291 A.2d 825, *cert. denied,* 409 U.S. 1090 (1972). For a discussion of this case, see notes 132-36 and accompanying text *infra.*

[6] *Id.* at 534-42, 291 A.2d at 833-37.

[7] *Id.* New Jersey's minimization statute is N.J. STAT. ANN. § 2A:156A-12(f) (1971). For a discussion of this statute and the recent amendments, see notes 131-32 *infra.* Under standard constitutional law, Dye's request for suppression would be denied for lack of standing; the rights in question belonged to the bar patrons, not to Dye. *See, e.g.,* Alderman v. United States, 394 U.S. 165 (1969), where the Court stated: "The established principle is that suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of the damaging evidence." *Id.* at 171-72. Courts ruling on minimization have generally ignored the standing problem, however, and have assumed that Title III creates a suppression remedy that overcomes lack of standing. *See* note 184 *infra.*

[8] 18 U.S.C. §§ 2510-2520 (1970).

[9] Although 24 jurisdictions have statutes authorizing wiretapping, the federal statute is binding on the states through the supremacy clause of the Constitution. The states have generally ruled that their wiretapping laws are not completely preempted by the federal statute, but rather that Title III, now codified in 18 U.S.C. §§ 2510-2520 (1970), sets minimum standards for state wiretapping legislation, and that states may choose to be more restrictive in authorizing wiretapping. *See* People v. Conklin, 12 Cal. 3d 259, 271, 522 P.2d

decisions of state and federal courts provide no clear picture of how to conduct a wiretap. A careful law-enforcement officer who read all the cases could only conclude that sometimes the courts have enforced the minimization requirement strictly and literally and sometimes the courts have been flexible and permissive.

Minimization is not the only problem that law-enforcement officers face in the use of wiretaps. This Comment treats the four most significant legal problems encountered in the execution of a court-authorized wiretap: minimization, amendment of the wiretap order, sealing the tapes upon termination of surveillance, and service of inventories on interested parties. As with the minimization problem, the decisions in the other three areas fail to provide a clear guide to proper wiretap procedure. This Comment is an effort to derive from the cases standards by which to evaluate police conduct in the use of wiretaps. Where the cases conflict or seem wrongly decided, an effort is made to resolve the conflict, to suggest different results, and to map for law enforcement officials the contours of what the courts most probably will and will not permit.

I

MINIMIZATION

A. *Conceptual Background*

In 1928 the first Supreme Court opinion to consider the wiretap problem declared that the fourth amendment did not apply because a wiretap did not entail a physical trespass.[10] The Court's thinking has become far more sophisticated since then,

1049, 1057, 114 Cal. Rptr. 241, 249, *appeal dismissed,* 419 U.S. 1064 (1974); Commonwealth v. Vitello, 327 N.E.2d 819, 833, 835 (Mass. 1975); State v. Siegel, 266 Md. 256, 292 A.2d 86 (1972). The 24 jurisdictions and their respective statutes are: 18 U.S.C. §§ 2510-20 (1970); ARIZ. REV. STAT. ANN. §§ 13-1051 to -1061 (Supp. 1973); COLO. REV. STAT. ANN. §§ 16-15-101 to -104, 18-9-301 to -310 (1973); CONN. GEN. STAT. ANN. §§ 53a-187 to -189, 54-41a to -41s (Supp. 1975); DEL. CODE ANN. tit. 11, §§ 1335-36 (1974); D.C. CODE ANN. §§ 23-541 to -556 (1973); FLA. STAT. ANN. §§ 934.01-.10 (Supp. 1975); GA. CODE ANN. §§ 26-3001 to -3010 (1972); KAN. STAT. ANN. §§ 22-2514 to -2519 (1974); MD. ANN. CODE C.J. §§ 10-401 to -408 (1974); MASS. GEN. LAWS ANN. ch. 272, § 99 (Supp. 1974); MINN. STAT. ANN. §§ 626A.01-.23 (Supp. 1975); NEB. REV. STAT. §§ 86-701 to -707 (1971); NEV. REV. STAT. §§ 179.410-.515, 200.610-.690 (1973); N.H. REV. STAT. ANN. §§ 570-A:1 to -A:11 (1974); N.J. STAT. ANN. §§ 2A:156A-1 to -26 (1971); N.M. STAT. ANN. §§ 40A-12-1.1 to -1.10 (Supp.1973); N.Y. CRIM. PRO. LAW §§ 700.05-.70 (McKinney 1971), N.Y. PENAL LAW §§ 250.00-.20 (McKinney 1967); ORE. REV. STAT. §§ 141.720-.990 (1974); R.I. GEN. LAWS ANN. §§12-5.1-1 to -16 (Supp. 1974); S.D. COMPILED LAWS ANN. § 23-13A-1 to -11 (Supp. 1974); VA. CODE ANN. §§ 19.1-89.1 to -89.10 (Supp. 1975); WASH. REV. CODE ANN. §§ 9.73.030-.100 (Supp. 1974); WIS. STAT. ANN. §§ 968.27-.33 (Supp. 1975).

[10] Olmstead v. United States, 277 U.S. 438 (1928).

however, and more recent opinions transcend the technical definitions of "search" and "seizure" in order to apply the fourth amendment's restraints to wiretap investigations.[11]

The modern premise that a wiretap in some way constitutes a search and seizure is now so well accepted that it is easy to forget that the Court might not have applied the fourth amendment at all. Wiretapping is more like an investigation than a search: it is a police technique to explore conspiracies that are impervious to normal methods of law enforcement.[12] Unlike a search and seizure situation, the officer applying for an eavesdropping order often has only a vague idea of the type of conversation he is seeking. Whereas the search and seizure often ends an investigation by providing the needed evidence, a wiretap is often used at the beginning of an investigation to identify suspects and to explore the extent of conspiracies. Moreover, the eavesdropping order itself often specifies that its purpose is investigatory and that the tap should not terminate when incriminating evidence is first discovered.[13]

---

[11] *Id.* (fourth amendment does not prohibit wiretapping unless there is a physical trespass); Goldman v. United States, 316 U.S. 129 (1942) (fourth amendment not violated by listening device placed against outside of a wall because there was no trespass); Silverman v. United States, 365 U.S. 505 (1961) (bug involving trespass violated fourth amendment, but result held not to rest on technicalities of local trespass law); Wong Sun v. United States, 371 U.S. 471 (1963) (verbal evidence may be a "fruit" of official illegality and thus subject to suppression); Lopez v. United States, 373 U.S. 427 (1963) (agent could record his own conversation with suspect without violating the fourth amendment); Osborn v. United States, 385 U.S. 323, 329-31 (1966) ("precise and discriminate" procedures limiting court-authorized bug did not violate fourth amendment); Berger v. New York, 388 U.S. 41 (1967) (New York law authorizing wiretapping struck down for failure to provide safeguards to keep wiretap from becoming general search); Katz v. United States, 389 U.S. 347 (1967) (otherwise valid bug invalidated by lack of prior judicial approval as required by fourth amendment warrant clause). *See generally* Cranwell, *Judicial Fine-Tuning of Electronic Surveillance*, 6 SETON HALL L. REV. 225, 227-43 (1975).

[12] *See generally* AMERICAN BAR ASSOCIATION PROJECT ON MINIMUM STANDARDS FOR CRIMINAL JUSTICE, STANDARDS RELATING TO ELECTRONIC SURVEILLANCE, Approved Draft, 1971, 13-98 [hereinafter cited as A.B.A. MINIMUM STANDARDS].

> The President's Commission on Law Enforcement and Administration of Justice has said that "the American system was not designed with Cosa Nostra-type criminal organizations in mind, and it has been notably unsuccessful to date in preventing such organizations from preying on society." The commission concluded, too, that only "in New York have law enforcement officials achieved some level of continuous success in bringing prosecutions against organized crime." The success was attributed "primarily to a combination of dedicated and competent personnel and adequate legal tools." Electronic surveillance techniques were termed "*the* tools."

Id. at 75-76 (emphasis in original).

[13] 18 U.S.C. § 2518(4) (1970) provides:

> (4) Each order authorizing or approving the interception of any wire or oral communication shall specify—

Much of the conceptual difficulty surrounding wiretap law stems from this basic source—the technique is by its very nature investigatory and bears only a rough resemblance to a traditional search for tangible evidence. Yet the fourth amendment is held to govern, and a modern method of electronic investigation must be shoehorned into the centuries-old categories of search and seizure.[14]

The minimization problem arises from this initial tension. Wiretapping is imprecise because in the normal case the monitoring agent does not know exactly what he is going to hear until he hears it.[15] Thus most agents have been reluctant to unplug their earphones for fear that they will miss an important conversation.[16] But the fourth amendment restricts the scope of the search and commands that only those things described in the warrant may be seized.[17] In a search for tangible evidence, an object improperly seized is simply returned to its owner; but a conversation, once intercepted, can never truly be returned.[18] The monitoring agent must therefore strive to intercept only those conversations described in the order. Perfection in this regard is unattainable because portions of irrelevant talk will always be heard before an agent determines that a conversation is outside the scope

. . . .

(e) . . . a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

This section gives the authorizing judge the flexibility to make the tap self-terminating if evidence against a group of individuals is all that is desired, or to permit the tap to continue in an investigatory posture after enough evidence to secure convictions has been obtained.

[14] Justice Black, dissenting in Berger v. New York, 388 U.S. 41 (1967) believed the fourth amendment should not be stretched to cover wiretapping:

> [T]he Amendment only bans searches and seizures of "persons, houses, papers and effects." This literal language imports tangible things. . . . It simply requires an imaginative transformation of the English language to say that conversations can be searched and words seized.

Id. at 78.

[15] *See, e.g.*, United States v. King, 335 F. Supp. 523, 541 (S.D. Cal. 1971), *rev'd on other grounds*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974); United States v. LaGorga, 336 F. Supp. 190, 196 (W.D. Pa. 1971).

[16] One court sharply criticized this tendency. "By justifying blanket surveillance on the ground that something relevant might turn up at any moment, the requirement of minimization would be rendered nugatory and the right of privacy nonexistent." United States v. King, 335 F. Supp. 523, 541 (S.D. Cal. 1971).

[17] The Supreme Court stated in Marron v. United States, 275 U.S. 192 (1927):

> The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.

Id. at 196.

[18] United States v. Focarile, 340 F. Supp. 1033, 1047 (D. Md.), *aff'd on other grounds sub nom.* United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), *aff'd*, 416 U.S. 505 (1974).

of his warrant and should not be monitored.[19] The fourth amendment bars only unreasonable searches and seizures, and it seems reasonable to expect that some innocent conversations will be picked up.[20] But since such conversations are outside the scope of the warrant, the agent assumes a duty to make a reasonable effort to minimize the number of innocent conversations he searches and seizes.[21] An agent who makes no effort to do so would cause the search to be unreasonable as a matter of constitutional law and the evidence would be suppressed.[22]

The Supreme Court's opinion in *Berger v. New York*[23] supports the view that minimization is a constitutional requirement.[24] In explaining its reasons for striking down a permissive New York wiretap authorization law, the court stated:

> [T]he statute's failure to describe with particularity the conversations sought gives the officer a roving commission to "seize" any and all conversations. It is true that the statute

[19] United States v. Scott, 516 F.2d 751, 754 (D.C. Cir. 1975); United States v. Bynum, 360 F. Supp. 400, 409 (S.D.N.Y.), *aff'd*, 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974).

[20] United States v. Scott, 516 F.2d 751, 754 (D.C. Cir. 1975).

[21] [The Statute] . . . requires the intercept procedure to be conducted so as to reduce to the smallest possible number the interception of "innocent" calls. In this context the word "possible" means "feasible" or "practicable" while still allowing the legitimate law enforcement aims of the statute to be accomplished. This is but another way of saying that the methods and efforts utilized in minimization must be reasonable, the traditional and acceptable standard of measuring the validity of a search under the Fourth Amendment.

United States v. Focarile, 340 F. Supp. 1033, 1047 (D. Md. 1972).

[22] In Kremen v. United States, 353 U.S. 346 (1957), F.B.I. agents arrested petitioners at a secluded cabin and proceeded to conduct a search incident to the arrest. The search was exhaustive, and the agents literally seized and removed the entire contents of the cabin. The Court stated: "The seizure of the entire contents of the house and its removal some two hundred miles away to the F. B. I. offices for the purpose of examination are beyond the sanction of any of our cases." *Id.* at 347. Although the Court approved seizure of items from the persons of the defendants, the scope of seizure was otherwise so broad that the entire search and seizure was vitiated and the items seized should not have been received in evidence.

The clear implication of this case is that if a monitoring agent makes no effort to limit seizures to the conversations described in the warrant, the search and seizure will be entirely void, and the evidence so obtained will be unusable in a prosecution of any of the defendants whose rights have been violated.

A recent case from the District of Columbia Circuit suggests, however, that a search and seizure may be reasonable even when the agent makes no effort to minimize. In United States v. Scott, 516 F.2d 751 (D.C. Cir. 1975), the court declined to suppress the wiretap evidence even though the government admittedly had intercepted all calls and had made no effort to minimize. The court found that interception of all calls would have been reasonable in the circumstances of the case, and that the agents' subjective intent was of no importance. *See* note 110 *infra*.

[23] 388 U.S. 41 (1967).

[24] *But see* Note, *Minimization: In Search of Standards*, 8 SUFFOLK U.L. REV. 60, 63 (1973).

> requires the naming of "the person or persons whose communications, conversations or discussions are to be overheard or recorded. . . ." But this does no more than identify the person whose constitutionally protected area is to be invaded rather than "particularly describing" the communications, conversations, or discussions to be seized. As with general warrants this leaves too much to the discretion of the officer executing the order.[25]

The monitoring officer, apparently, may not be given a "roving commission" to seize what he desires. The warrant must limit him to particular conversations, and he must limit himself to seizing what is described or the warrant would be meaningless.

In striking down the New York statute, *Berger* also laid out a blueprint for a constitutional wiretapping statute.[26] The Supreme Court clarified its views the following year in *Katz v. United States,*[27] and Congress responded with Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[28] Title III outlaws private wiretapping[29] and establishes rigorous standards governing applications for a wiretap. The application is required to demonstrate that probable cause exists to believe that (*1*) one of an enumerated list of crimes has been, is being, or will be committed; (*2*) particular communications concerning that crime will be obtained; and (*3*) the facilities to be tapped are being used in connection with commission of the crime.[30] The order, or warrant,

[25] 388 U.S. at 59.

[26] The statute was struck down because it did not clearly require a showing of probable cause that evidence of a crime would be obtained, the eavesdropping order was not required to describe with particularity the place to be searched or the persons or things to be seized, the time limits on tbe wiretap were vague and excessively long, and the statute did not require notice to persons whose conversations had been seized. At the same time, the Court very plainly implied that if the defects in the New York statute were corrected, the resulting statute would pass constitutional muster.

[27] 389 U.S. 347 (1967).

[28] 18 U.S.C. §§ 2510-2520 (1970). The legislative history of Title III, contained in the senate report, states forthrightly that the statute was drafted specifically in response to *Berger* and *Katz.* S. REP. No. 1097, 90th Cong., 2d Sess. 66 (1968), *reprinted,* U.S.C.C. & A.N. 2112, 2153 (1968) [hereinafter cited as LEGISLATIVE HISTORY]. Although the Supreme Court has not yet passed on the question, the courts that have considered Title III have overwhelmingly declared it constitutional. *Accord,* United States v. James, 494 F.2d 1007 (D.C. Cir. 1974), *cert. denied,* 419 U.S. 1020 (1975); United States v. Cafero, 473 F.2d 489 (3d Cir. 1973), *cert. denied,* 417 U.S. 918 (1974); United States v. Bobo, 477 F.2d 974 (4th Cir. 1973); United States v. Tortorello, 480 F.2d 764 (2d Cir.), *cert. denied,* 414 U.S. 866 (1973); United States v. Cox, 462 F.2d 1293 (8th Cir. 1972), *cert. denied,* 417 U.S. 918 (1974); United States v. Cox, 449 F.2d 679 (10th Cir. 1971), *cert. denied,* 406 U.S. 934 (1972). *Contra,* United States v. Whitaker, 343 F. Supp. 358 (E.D. Pa. 1972), *rev'd,* 474 F.2d 1246 (3d Cir.), *cert. denied,* 412 U.S. 953 (1973).

[29] 18 U.S.C. § 2511 (1970).

[30] *Id.* § 2518(3).

issued when the application is approved must specify the identity of the person, if known, whose communications are to be intercepted; the nature and location of the facilities to be tapped; the type of communication sought and the crime to which it relates; the period of time for which the tap is authorized; and whether or not the tap is to terminate automatically when the type of communication sought is first intercepted.[31]

Title III also provides standards for the conduct of wiretaps, and includes an explicit minimization rule:

> Every order and extension thereof shall contain a provision that the authorization to intercept shall be . . . conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter.[32]

This section expressly commands the monitoring officer to minimize interceptions of "innocent"[33] conversations and gives the minimization rule statutory, as well as constitutional, dimension. A critical threshold question immediately arises, however. Although the constitutional analysis showed that the thing to be minimized is the search and seizure of innocent conversations,[34] the statute uses the word interception throughout. What, then, is an interception?

Although the statute itself defines interception as "aural acquisition"[35]—literally, to come into possession through the sense of hearing—this definition offers little guidance. The agent on the spot must know whether he is required to minimize the number of innocent conversations overheard, recorded, transcribed, or disclosed, and it is not obvious which of these constitute an aural

---

[31] *Id.* § 2518(4).

[32] *Id.* § 2518(5). The statute further provides:

> The contents of any wire or oral communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any . . . communication . . . shall be done in such way as will protect the recording from editing or other alterations.

Id. § 2518(8)(a).

[33] An innocent conversation is one which should not be intercepted because it is outside the scope of the warrant. For a discussion of what conversations may be properly intercepted, see notes 70-82 and accompanying text *infra.*

[34] *See* notes 17-26 and accompanying text *supra.*

[35] 18 U.S.C. § 2510(4) (1970). The aural acquisition must also be through the use of some electronic, mechanical, or other device, so that simple overhearing of a conversation via the naked ear is not an interception. This provision flows from the constitutional premise that the use of searchlights or fieldglasses to observe activity that is out in the open does not constitute a search under the fourth amendment. United States v. Lee, 274 U.S. 559, 563 (1927); Fullbright v. United States, 392 F.2d 432, 433 (10th Cir. 1968).

acquisition.[36] Since an agent cannot properly comply with the statute unless he knows what to minimize, it is surprising to note that there has been little judicial effort to define the term "interception"; in fact, most courts seem to have been unaware that a question exists. As a result, the courts have used the term to mean different things, and there is little uniformity even among the federal decisions. One New York court apparently held that recording alone constitutes an interception;[37] a federal district court adopted an "overhearing" definition;[38] and a federal court of appeals indicated that the interception takes place when the tapes are transcribed or disclosed.[39]

The disagreement among the courts is not surprising, for the statute is ambiguous. Some writers point to the section of Title III that directs that all interceptions should also be recorded and infer from this language that "interception" cannot be synonymous with "recording."[40] It seems likely, however, that the purpose of this section was to avoid the situation in which a monitor overhears incriminating evidence but fails to record it, leaving the defendant

[36] In instructing its own attorneys in how to run a wiretap, the Department of Justice has stated candidly that it does not really know what "aural acquisition" means. The Department's wiretap instruction manual, the contents of which were kept secret for several years, states: "[I]t is not . . . clear what is intended to be included in the terms 'aural acquisition' . . . ." U. S. DEPARTMENT OF JUSTICE, MANUAL FOR CONDUCT OF ELECTRONIC SURVEILLANCE 1 (1970) [hereinafter cited as JUSTICE DEPT. MANUAL].

"Aural acquisition" alone might indicate that interception is overhearing since the human faculty of hearing is not exercised when a tape recorder stores a conversation. But in a broader sense, the machine is hearing the conversation and making a permanent record for others to hear; the machine has "acquired" the conversation through an "aural" mechanism. "Acquisition" can be construed in an even broader sense to mean use of, or exercise of dominion over. In that case, interception might not occur until the tape had been transcribed, *i.e.*, transformed into readily usable form, or even offered in evidence.

[37] People v. Castania, 73 Misc. 2d 166, 172, 340 N.Y.S.2d 829, 835 (County Ct. 1973).

[38] United States v. Bynum, 360 F. Supp. 400, 409 (S.D.N.Y.), *aff'd*, 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974).

[39] In United States v. Bynum, 475 F.2d 832 (2d Cir. 1973), the Second Circuit noted: "The mischief lies in the interception obviously and what was not transcribed remains unknown." *Id.* at 837. The implication seems to be that if it was not transcribed, it was not intercepted.

On remand the district court adopted the "overhear" definition. 360 F. Supp. at 409. In the court of appeals for the second time, the court recognized the definitional problem and ducked it: "We need not determine, however, whether the interception prohibited by the statute is aural intrusion or mechanical recordation." 485 F.2d 490, 502 (2d Cir. 1973).

[40] 18 U.S.C. § 2518(8)(a) (1970). See note 32 and accompanying text *supra* for text of the statute. *See also* United States v. Bynum, 360 F. Supp. 400, 408-09 (S.D.N.Y.), *aff'd*, 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds*, 417 U.S. 903 (1974); Note, *Minimization: In Search of Standards*, 8 SUFFOLK U.L. REV. 60, 70 (1973). At best, this analysis shows that "interception" is not the same as "recording," but it cannot identify the "true" definition of interception. At worst, this analysis misconstrues the intent of Congress. *See* note 41 and accompanying text *infra*.

no way to attack the agent's recollection at trial.[41] The statute does not provide for the reverse situation in which the agent records a conversation but does not overhear it at the time. In fact, the statute shows no awareness at all of the problem which is created by the use of the word "interception."

If the draftsmen had considered which part of the wiretapping process was to constitute an interception, they certainly would have specified their intent in the statute.[42] The rest of the statute is painstakingly written, and the only conclusion that may be drawn from the omission is that Congress did not consider the question at all.

Although the statute provides no guidance as to the proper meaning of "interception," minimization is a constitutional requirement and the fourth amendment should therefore yield a working definition. A careful application of traditional search and seizure law, however, results in no better than shaky conclusions.

According to pre-Title III doctrine, a search is said to differ from a seizure in that a search is defined as a perception of a quantity of things, among which are the items to be seized,[43] while a seizure is an exercise of dominion over the items that have been located in the search.[44] Both search and seizure must be reasonable.[45] The scope of the search is reasonable if it goes no further than is necessary to find the items specified in the warrant.[46] For example, an officer searching for a car may do no more than glance into areas that could hide a car; he may not look in drawers or closets. Similarly, an officer searching for a revolver may search all places that could hide a revolver; he may search in drawers and closets, but he may not poke pins in tubes of toothpaste or open envelopes to read the contents. The scope of a seizure is reasonable if it does not exceed the items described in the warrant plus other evidence that is in plain view during the search.[47]

---

[41] The legislative history to § 2518(8)(a) merely paraphrases the statute and gives no clue to the draftsmen's intent. The same is true of the minimization section, § 2518(5). LEGISLATIVE HISTORY 2192-93.

[42] The Supreme Court used this same method of statutory analysis in interpreting a different section of Title III in United States v. Kahn, 415 U.S. 143, 152-53 (1974).

[43] *See* Berger v. New York, 388 U.S. 41, 97-100 (1967) (dissenting opinion, Harlan, J.).

[44] *Id.*

[45] *See* Go-Bart Importing Co. v. United States, 282 U.S. 344, 356-57 (1931); Boyd v. United States, 116 U.S. 616, 641 (1886) (concurring opinion, Miller, J.); Note, *Minimization and the Fourth Amendment,* 19 N.Y.L.F. 861, 868-74 (1974).

[46] *Cf.* Chimel v. California, 395 U.S. 752 (1969).

[47] Coolidge v. New Hampshire, 403 U.S. 443, 465-68 (1971).

Thus both search and seizure must be minimized—search, because it must be limited to a search for seizable items, and seizure, because it must be limited to the items in the warrant. This result is not easily transferred to the wiretap context; for it is surely not obvious which parts of the surveillance process correspond to a search and which parts to a seizure. Two dissenting opinions in *Berger* address this problem. Justice White reasoned that a monitoring agent is only searching when he overhears or records conversations:

> Petitioner suggests that the search is inherently overbroad because the eavesdropper will overhear conversations which do not relate to criminal activity. But the same is true of almost all searches of private property which the Fourth Amendment permits. In searching for seizable matters, the police must necessarily see or hear, and comprehend, items which do not relate to the purpose of the search. That this occurs, however, does not render the search invalid . . . so long as the police, in executing that warrant, limit themselves to searching for items which may constitutionally be seized.[48]

He added in a footnote that "[r]ecording an innocent conversation is no more a 'seizure' than occurs when the policeman personally overhears conversation while conducting a search with a warrant."[49] Justice Harlan agreed and concluded that seizure of a conversation must be something beyond overhearing or recording:

> [I]n my view, conversations are not "seized" either by eavesdropping alone, or by their recording so that they may later be heard at the eavesdropper's convenience. Just as some exercise of dominion, beyond mere perception, is necessary for the seizure of tangibles, so some use of the conversation beyond the initial listening process is required for the seizure of the spoken word.[50]

Justice White would equate overhearing with a search. Since a search must be minimized, overhearing must also be minimized. Justice Harlan would equate a seizure with "some use of the conversation."[51] Since seizure must be minimized, uses such as transcription of the tapes or disclosure of their contents presumably must also be minimized. According to both Justices, recording alone is not a seizure. But neither Justice explains what

---

[48] 388 U.S. at 108 (dissenting opinion, White, J.).

[49] *Id.*

[50] *Id.* at 98 (dissenting opinion, Harlan, J.). Harlan's and White's reasoning was followed in United States v. Bynum, 360 F. Supp. 400, 408-09 n.7 (S.D.N.Y. 1973).

[51] 388 U.S. at 98.

recording alone *is*. It is not necessarily a search, for the tape may never be played back and no human ear will ever hear the conversation.[52] But if recording is also not a seizure, then what is it?

The analogy between wiretapping and search and seizure thus breaks down in its details, and any effort to make the comparison results in anomalies that belie the technique. Moreover, the majority opinions of the Supreme Court in the wiretap cases have made no effort to make the specific analogy and have used the fourth amendment only in a vague, conclusory fashion.[53]

A wiretap simply does not fit into the ancient conceptual categories. It is not a two-step process of perception and acquisition as is a search for tangible items. Wiretapping more accurately takes place all at once; the words are heard and recorded and the process is complete. Preparing the tapes for use by transcribing them is not logically necessary and is really an additional and separate act. "Search" and "seizure" are inadequate terms to describe the process of wiretapping. The definition of interception, therefore, will be found neither by analyzing the Supreme Court's interpretations of search and seizure nor by analyzing the statute.[54] The Supreme Court has decided that the fourth amendment governs and the best way to define interception is to take the broad perspective and ask what definition will, as a matter of policy and practicality, best effect the purpose of Title III and the fourth amendment.[55] The Court in *Katz* rephrased the fourth amendment

---

[52] *Cf.* State v. Dye, 60 N.J. 518, 528-37, 291 A.2d 825, 830-34, *cert. denied,* 409 U.S. 1090 (1972) (continuous recording violates neither the statute nor the Constitution; implies strongly that seizure occurred when the guilty conversations were picked out of the continuous tape and transcribed onto a "work copy"). For a discussion of this case, see notes 132-36 and accompanying text *infra.*

[53] In *Berger,* the Court avoided defining search or seizure in the wiretapping context: "[O]ur subsequent cases . . . found 'conversation' was within the Fourth Amendment's protections, and that the use of electronic devices to capture it was a *'search'* within the meaning of the Amendment. . . ." 388 U.S. at 51 (emphasis added). "Likewise the statute's failure to describe with particularity the conversations sought gives the officer a roving commission to *'seize'* any and all conversations." *Id.* at 59 (emphasis added). The Court's opinion in *Katz* was equally imprecise: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied . . . and thus constituted a *'search and seizure'* within the meaning of the Fourth Amendment." 389 U.S. at 353 (emphasis added). The Court's opinions thus offer little assistance in an analysis of wiretapping in search and seizure terms.

[54] *See* notes 35-42 and accompanying text *supra.*

[55] The legislative history shows that Congress intended the ultimate aim of Title III to be the preservation of privacy consistent with effective law enforcement. The legislative history states in the introduction:

> Title III has as its dual purpose (1) protecting the privacy of wire and oral

to protect an individual's reasonable expectation of privacy against unreasonable intrusion,[56] and thus the proper definition of "interception" is the one that will best protect that expectation.

Overhearing is the very heart of invasion of privacy; unknown to the parties conversing, a silent third party is listening to what is thought to be private. "Interception" at a minimum must cover overhearing.[57] A conversation that is both overheard and recorded is therefore also intercepted. The problem case is the conversation that is recorded but not simultaneously overheard, for as long as the tape is not played back, the contents of the conversation remain known only to the original participants.

As a matter of policy, however, mere recording should also be held to constitute interception.[58] A conversation, once recorded, may be replayed at will. A monitoring agent has little incentive to be selective when he listens to a tape, and particularly if he can locate a private place to play it back, he will always be tempted to listen to everything to ensure that no incriminating conversations were missed.[59] No one can tell exactly which parts of a recorded tape have been played back and which parts remain secret, and if the replaying was done privately, a court must rely on the agent's unsupported word as to which parts he replayed. The person transcribing the tape will inevitably listen to parts that are

communications, and (2) delineating ou a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.

LEGISLATIVE HISTORY 2135. *See also* United States v. Tortorello, 480 F.2d 764, 784 (2d Cir.), *cert. denied,* 414 U.S. 866 (1973).

[56] 389 U.S. at 350-53.

[57] The Department of Justice believes that overhearing constitutes an interception. The wiretap instruction manual which the department distributes to attorneys who supervise wiretaps states:

> [T]he desirability of recording the intercepted communication is obvious. Since evidence of the intercepted conversation would be admissible in future trials it is preferable to produce the verbatim recording rather than relying solely on the memory of the agent who *overheard* the conversation.

JUSTICE DEPT. MANUAL 28 (emphasis added).

[58] See the persuasive discussion in Note, *Minimization of Wire Interception: Presearch Guidelines and Postsearch Remedies,* 26 STAN. L. REV. 1411, 1415-17 (1974).

[59] In United States v. Bynum, 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds,* 417 U.S. 903 (1974), the court noted the appellant's argument that recording should constitute an interception:

> Appellants respond that the statute was never intended to permit recordation of all conversations. Such a construction would, in their view, allow the Government or anyone else to legally create a tape library of the conversations of any citizen. If such reasoning were applied to the situation of a warrant covering tangible items, seizure of the contents of a whole house would be permissible, in their view, on the ground that to do so would prevent any destruction or disappearance of exculpatory evidence.

Id. at 502 n.6. The court did not decide the point, however. *See* note 39 *supra.*

irrelevant to the investigation, and others may hear the entire tape for any of several reasons.[60] Furthermore, if all conversations are recorded, but only some are overheard, the defendant has no means of challenging the agent's testimony that certain conversations were not overheard, aside from the agent's own logs.[61] If only those conversations which are overheard are recorded, however, the defendant has a taped record showing exactly which conversations were, in fact, intercepted.

Three years after the passage of Title III, the New York legislature amended its wiretap authorization law to conform to the federal statute. Presented with a chance to resolve the ambiguous Title III definition of interception, the legislature stated forthrightly, " 'Intercepted communication' means (a) a telephonic or telegraphic communication which was intentionally overheard or recorded . . . ."[62] This redefinition by a prestigious state legislature is a substantial factor militating in favor of a record-or-overhear interpretation.

The major problem with a rule making a recording constitute an interception is that the tapes resulting from the agents' switching the recorder off each time they stop listening are a fragmentary and incomplete record of the suspects' pattern of communications. The defendants may always charge that the wiretap was edited or that statements were taken out of context, and the government would have difficulty refuting the charge without a complete taped record.[63] Moreover, persons trying to pursue a civil remedy under section 2520 for illegal interception of their communications may need a complete, taped record as evidence in the suit.[64]

---

[60] The judge may listen to the tape, for instance, to get some idea of how it sounded when the agents first heard it, or to determine whether a claim that portions were difficult to understand is valid. The judge may use a representative to analyze the tapes for him, as in United States v. Bynum, 360 F. Supp. 400, 403 (S.D.N.Y. 1973), and both the defense and prosecution regularly prepare statistical analyses of the tapes after listening to every word of every tape. *See, e.g.*, United States v. King, 335 F. Supp. 523, 542 (S.D. Cal. 1971); United States v. Focarile, 340 F. Supp. 1033, 1049 (D. Md. 1972); United States v. Lanza, 349 F. Supp. 929, 932 (M.D. Fla. 1972).

[61] It has been federal practice for agents to keep logs of time, duration, and approximate content of each conversation intercepted. The procedure used in one investigation is described in detail in United States v. Falcone, 364 F. Supp. 877, 880 (D.N.J. 1973).

[62] N.Y. CRIM. PRO. LAW § 700.05(3) (McKinney 1971).

[63] United States v. Leta, 332 F. Supp. 1357, 1360 (M.D. Pa. 1971); State v. Dye, 60 N.J. 518, 539-40, 291 A.2d 825, 836, *cert. denied*, 409 U.S. 1090 (1972).

[64] For a discussion of the 18 U.S.C. § 2520 (1970) civil remedy, see notes 164-66 and accompanying text *infra*. Generally, § 2520 creates a cause of action accruing to a person

This difficulty could be overcome through the use of court-appointed representatives or a sealed, voice-actuated recorder to produce a complete taped record which was not at any time available to the monitoring agents or to the prosecution, and which would be sealed and never opened unless the defendants so moved.[65] Since this definition of interception is policy-based, it would not be troublesome to hold that the monitors' work-tapes constitute interceptions, but that a sealed complete set of tapes produced solely for the benefit of the defendants is not prohibited.

B. *The Scope of Interception*

Once the monitoring agent knows that a conversation is intercepted when it is overheard or recorded, he is ready to put the minimization principle into practice. Before he can properly do so, however, he must know what kinds of conversations he is not permitted to intercept.

The case law on this subject is comprehensive but inconsistent. It covers seven years of wiretapping practice under Title III, and as the minimization issue has been repeatedly litigated, the decisions have generally become increasingly sophisticated. Minimization practices have sharply improved,[66] and many

---

whose communications are illegally intercepted, used, or disclosed, against the person committing the violation.

[65] *See* notes 141-44 and accompanying text *infra*.

[66] In the first year of wiretapping under Title III little effort was made anywhere to comply with the minimization section. But when the federal courts began to suppress evidence as a result of the government's failure to minimize, the Department of Justice and its investigating attorneys rapidly became aware of the minimization problem and began to develop techniques to deal with it. *Cf.* JUSTICE DEPT. MANUAL 35-40 (little sensitivity to minimization as of 1970). Similar problems plagued state district attorneys. In an evaluation of the wiretap practices of the Kings County, New York, District Attorney, a report prepared by the National Wiretap Commission stated:

> [D]uring the period immediately following the enactment of the New York equivalent of Title III, the Kings County D.A. took few if any steps to insure [sic] that the non-consensual electronic surveillance utilized by his office were carried out in accordance with the demanding standards embodied in that legislation. By and large, the early taps which the [National Wiretap] Commission staff had the opportunity to review were marked by the kinds of sloppy practices with which the decisions in *Berger & Katz* were concerned and which the draftsman of Title III sought to prevent.
>
> . . . .
>
> . . . With the passage of time, however, the office apparently became more familiar with the requirements of the new statute and more professional in its utilization of the tool of electronic surveillance.

HEARINGS BEFORE THE NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE, *Staff Report on Kings County*, Tab C, at 5 (March 18-20, 1975). *Compare* United States v. Scott, 331 F. Supp. 233 (D.D.C. 1971), *vacated*, 504 F.2d 194 (D.C. Cir. 1974), *rev'd after remand*, 516 F.2d 751 (D.C. Cir. 1975) (no effort at minimization), *with* United States v. Falcone, 364 F. Supp. 877 (D.N.J. 1973), *aff'd*,

inconsistencies in the decisions reflect the rapid developments in practice.

Early cases simply marshalled the facts of the particular wiretap and then stated in conclusory fashion whether or not the government had properly minimized.[67] Unfortunately, none established comprehensive criteria for future cases. Later decisions recognized that no fixed rules could adequately deal with the vast array of different fact situations and that minimization would have to be dealt with on a case-by-case basis.[68] The latest and most sophisticated decisions identify the variables that determine in each case whether the government has properly minimized.[69]

On the most general level, an eavesdropping order allows interception of conversations that provide "evidence of" certain offenses.[70] The evidence may be such as would incriminate a specific individual,[71] or of a kind that would aid the investigators in perceiving the size, nature, identity and mode of operation of the criminal enterprise.[72] Conversations that are irrelevant to the investigation generally are not to be intercepted.[73] These would include innocent conversations between known suspects,[74] most

505 F.2d 478 (3d Cir. 1974), *cert. denied,* 420 U.S. 955 (1975) (comprehensive minimization plan developed).

[67] *See, e.g.,* United States v. Scott, 331 F. Supp. 233 (D.D.C. 1971).

[68] *See, e.g.,* United States v. Bynum, 360 F. Supp. 400, 410 (S.D.N.Y. 1973).

[69] *See, e.g.,* United States v. Scott, 516 F.2d 751, 758-59 (D.C. Cir. 1975); United States v. Armocida, 515 F.2d 29, 44 (3d Cir. 1975); United States v. James, 494 F.2d 1007, 1019-21 (D.C. Cir. 1974), *cert. denied,* 419 U.S. 1020 (1975).

[70] 18 U.S.C. § 2516(1) (1970).

[71] *See, e.g.,* United States v. Kahn, 415 U.S. 143 (1974); United States v. Sklaroff, 323 F. Supp. 296 (S.D. Fla. 1971), *aff'd,* 506 F.2d 837 (5th Cir. 1975) (wiretaps used to develop evidence on known suspects operating single bookmaking operations).

[72] *See, e.g.,* United States v. Bynum, 360 F. Supp. 400, 404 (S.D.N.Y. 1973) (far-flung narcotics conspiracy).

[73] A clearly irrelevant conversation cannot provide "evidence of" a crime and is therefore outside the scope of lawful interception under 18 U.S.C. § 2516(1) (1970).

[74] *But see* United States v. Bynum, 360 F. Supp. 400 (S.D.N.Y. 1973); United States v. King, 335 F. Supp. 523, 542 (S.D. Cal. 1971). The *Bynum* court stated: "[C]alls between known co-conspirators should be monitored, for relevant information may emerge at any point in a call." 360 F. Supp. at 416.

This may be true where the co-conspirators are engaged in criminal enterprise on a full-time basis, and the agent may reasonably expect that any call between conspirators will be in furtherance of the aims of the conspiracy. But if the conspirators are only fringe members of the criminal enterprise and they are also social acquaintances, their calls to each other may only infrequently touch on criminal matters, and the agents would definitely not be justified in intercepting all interconspirator conversations.

As in *Bynum,* the courts have tended to state dogmatically that all calls between conspirators may be intercepted, but like other minimization rules, this one really should depend on the facts and circumstances of each case. *See* notes 83-110 and accompanying text *infra.*

conversations involving a third party known not to be involved in the criminal enterprise,[75] nearly all conversations involving two people known not to be involved,[76] and all privileged conversations.[77] By specific statutory provision, conversations producing evidence of offenses other than those specified in the warrant may be intercepted, provided that the monitoring agents apply for an amendment to the original warrant as soon as possible.[78]

Beyond these initial generalities, few ironclad rules exist. When the suspects were aware that their phones were tapped, and so spoke in a difficult code, the agents were held to be justified in intercepting nearly every conversation.[79] But when the monitoring agents intercepted the suspect's wife speaking to local merchants, and his family speaking to their friends, the court held that the agents did not have the right to intercept all conversations.[80]

Defining the scope of permissible interception really entails a two-step process of analysis. The first is determining which conversations are proper subjects for interception, and the second is determining how much leeway to allow agents who intercept more than is strictly proper before decreeing a failure to minimize.

1. *Interception of Nonpertinent Conversations*

Partly because in retrospect it is often easy to separate pertinent conversations from nonpertinent ones,[81] the courts have made almost no effort to arrive at a working definition of what constitutes a pertinent conversation. Nevertheless, the cases show a strong inclination to find pertinent any conversation that has any

[75] Where the conversation with the uninvolved third party has provided pertinent information, however, the courts have tended to allow interception. *See, e.g.,* United States v. Falcone, 364 F. Supp. 877, 882-83 (D.N.J. 1973). *See* note 82 *infra.*

[76] United States v. Scott, 516 F.2d 751, 755 (D.C. Cir. 1975); United States v. Sisca, 361 F. Supp. 735, 744 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1008 (1974).

[77] *See* 18 U.S.C. § 2517(4) (1970) (privileged communications do not lose their privileged character when they are intercepted); United States v. Kahn, 471 F.2d 191 (7th Cir. 1972), *rev'd on other grounds,* 415 U.S. 143 (1974) (certain husband-wife conversations are not privileged and are therefore subject to interception); JUSTICE DEPT. MANUAL 35-38. *See* notes 111-21 and accompanying text *infra.*

[78] 18 U.S.C. § 2517(5) (1970). *See* notes 167-221 and accompanying text *infra.*

[79] United States v. Bynum, 360 F. Supp. 400, 412-13 (S.D.N.Y. 1973).

[80] United States v. Sisca, 361 F. Supp. 735, 744 (S.D.N.Y. 1973).

[81] At the time of interception, however, it can be very difficult indeed to discriminate between pertinent and nonpertinent conversations. *See, e.g.,* United States v. Capra, 501 F.2d 267, 273-74 (2d Cir. 1974), *cert. denied,* 420 U.S. 990 (1975). *See* note 99 *infra.*

conceivable connection to the investigation, no matter how remote.[82]

The issue in the minimization cases, however, is usually not which conversations were pertinent. The dispute more often centers on whether the agents have intercepted too many nonpertinent conversations. More accurately stated, the question has two prongs. First, how freely may agents intercept conversations that very clearly were not going to provide evidence—obviously innocent calls. Second, how freely may agents intercept conversations that appear at the time to be in the gray area between clearly relevant and clearly irrelevant in the hope that the conversation will take a pertinent turn or will later seem pertinent in the light of new information.

Although the question should be split into these two

[82] In United States v. Falcone, 364 F. Supp. 877 (D.N.J. 1973), *aff'd*, 505 F.2d 478 (3d Cir. 1974), *cert. denied*, 420 U.S. 955 (1975), for instance, the court held that interception of many debatably pertinent calls was proper. The court allowed interception of calls to the telephone company (to find out whether telephone service was about to be discontinued), calls to travel agencies and airlines (to keep track of the movements of what was described as an international heroin ring), calls to a bank to procure money (because the money was needed to buy narcotics), and calls to persons who were not identified (since one purpose of the tap was to develop the extent and identity of the conspiracy). *Id.* at 882. A number of courts have stated in dicta that, because of the high probability that pertinent material will turn up, any conversation between known conspirators is automatically subject to interception, even if the talk appears to be confined to gossip. *See* note 74 *supra*. The court in *Falcone* went even further:

> It is appropriate to note at this juncture that [the special agent in charge] believed that a call between a conspirator and a clearly established non-conspirator was not as a rule to be recorded. I do not regard minimization under the statute or my Order as requiring this limited view. Conversations of this nature may often be highly significant to an investigation of a far flung and sophisticated conspiracy such as this is alleged to be. The non-conspirator may, in fact, become a conspirator in the near future or even during the very call being monitored. The non-conspirator may, however innocently, aid the other party in furtherance of an illegal objective by, for example, making travel arrangements, or arranging financial assistance for the illegal enterprise. Also . . . the conspirator may either volunteer information or respond to innocent questions with highly incriminating answers.

Id. at 883. This view seems excessively permissive. Protection of privacy is ignored and the law enforcement aspect dominates. Because of the remote possibility that the conspirator will volunteer incriminating information or that he will try to recruit the innocent party, the privacy of innocent citizens may be invaded under this view any time they receive a call from a conspirator. The legislative history of Title III shows that one of the primary purposes of the statute was to protect the privacy of wire and oral communications. *See* note 55 *supra*. The right to privacy clearly is not to be ignored every time there is an opportunity, no matter how remote, to obtain evidence. Title III does not guarantee that law enforcement officers will hear every pertinent word, regardless of how many innocent conversations are intercepted; indeed, that is the whole purpose of the minimization section. *See* United States v. King, 335 F. Supp. 523, 541 (S.D. Cal. 1971), *rev'd on other grounds*, 478 F.2d 494 (9th Cir. 1973), *cert. denied*, 417 U.S. 920 (1974). The court in *Falcone* has surely struck the balance between privacy and law enforcement in a manner inconsistent with the spirit of Title III.

components—interception of possibly pertinent and obviously nonpertinent calls—the courts have not done so explicitly, and the clarity of the case law has suffered for it. Different methods of evaluation should apply on the one hand to interception of possibly pertinent conversations which later turn out to be nonpertinent, and on the other hand to interception of conversations which were patently innocent from the beginning, such as a conversation involving nonconspirators using a pay telephone. The courts should generally be flexible and tolerant when dealing with the first kind of overage, and rigid and unbending when dealing with the second—the first kind of overage can be defended as a reasonable search for a seizable conversation, but the second cannot be so defended.

The courts have not drawn this distinction, however, and the cases can more practically be explained in a different way. There appear to be six variables which, when evaluated in the context of each case, account for most of the minimization decisions. Which variables apply will vary from case to case, and in some cases a single variable will be determinative.

(*1*) Objective of the wiretap. The objective of a wiretap may range from simple conviction of a known individual[83] to exploration of an unknown, far-flung conspiracy.[84] The courts have generally allowed a greater margin of error to agents conducting a more ambitious investigation and have found a wider range of calls to be pertinent.[85] In one complex investigation of a multi-state narcotics conspiracy, a federal district court held that monitoring agents were justified in intercepting 100 percent of the calls.[86] In a far more simple investigation, involving only a few suspects and a pay telephone, the court held agents to strict compliance with its minimization directive.[87]

(*2*) Location and use of the telephone. Sometimes a telephone is located in a headquarters used exclusively to direct

---

[83] *See, e.g.*, United States v. George, 465 F.2d 772 (6th Cir. 1972). *See also* cases cited in note 71 *supra*.

[84] *See* note 72 and accompanying text *supra*.

[85] *See* note 82 *supra*.

[86] United States v. Bynum, 360 F. Supp. 400 (S.D.N.Y. 1973). The conspiracy was also allegedly responsible for "murders, robberies, ('take-offs' of other drug dealers), thefts, possession of stolen property, the use of lethal weapons, bribery and the obstruction of justice." *Id.* at 404. The suspects had so thoroughly corrupted local law enforcement officials that outside agents had to be brought in to man the wiretap. *Id.* at 411. Moreover, the application for the warrant showed that a number of attorneys were deeply involved with the conspiracy. *Id.* at 404.

[87] United States v. George, 465 F.2d 772 (6th Cir. 1972).

criminal activities. Agents monitoring conversations over such a telephone may reasonably expect that virtually all conversations will be relevant and evidentiary.[88] In such cases the courts have allowed interception of almost any kind of conversation on the theory that any given conversation has a very high probability of being relevant, and any irrelevant calls are discouraged in order to keep the line available for business.[89] One district court even allowed interception of many conversations involving a babysitter at the headquarters who occasionally relayed messages from one conspirator to another.[90]

Other telephones may be located in family residences or in public places, such as bars or street corners, where agents must expect that evidentiary conversations will be overheard only when the suspect is using the telephone.[91] In these cases, a very high percentage of the calls is likely to be irrelevant, and the courts have liberally found failures to minimize unless the agents have made serious and conscientious efforts to screen out innocent conversations. The theory here has been that users of family or public telephones have a high expectation of privacy, and that monitoring agents must be correspondingly vigilant.[92] Interception of only a handful of private calls out of thousands of criminal ones emanating from a criminal headquarters is a de minimis problem, and users of such a telephone have little socially recognized expectation of privacy. Interception of a great many innocent calls involving people who have a high expectation of privacy in their homes or in phone booths, however, is a serious failure of minimization.

(*3*) Nature of the criminal enterprise. Where the subject matter of the conversations is inherently difficult to follow, as in many narcotics conspiracies, the courts have allowed agents

---

[88] United States v. James, 494 F.2d 1007, 1021-23 (D.C. Cir. 1974), *cert. denied,* 419 U.S. 1020 (1975); United States v. Bynum, 485 F.2d 490, 501 (2d Cir. 1973), *vacated on other grounds,* 417 U.S. 903 (1974).

[89] In one such case the court concluded:

> The telephones in this case were used almost exclusively to conduct illegal transactions; any personal conversations were mere specks in the torrent of conspiratorial communications. The appellants were not in a position to insist that their few legitimate personal remarks must be sieved out from the great volume of their unlawful conversations.

United States v. James, 494 F.2d 1007, 1023 (D.C. Cir. 1974).

[90] United States v. Bynum, 360 F. Supp. 400, 413 (S.D.N.Y. 1973).

[91] *See, e.g.,* United States v. George, 465 F.2d 772, 774 (6th Cir. 1972).

[92] United States v. George, 465 F.2d 772 (6th Cir. 1972); United States v. Sisca, 361 F. Supp. 735 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1008 (1974); United States v. LaGorga, 336 F. Supp. 190 (W.D. Pa. 1971).

considerable leeway in what they intercept. Most courts note that the agents' efforts at minimization must be evaluated by using the agents' own perspective; it is meaningless to argue after the fact that a large percentage of the intercepted conversations were innocent if the agents could not reasonably differentiate between innocent and guilty conversations at the time of interception.[93] The courts have emphasized that a search need only be reasonable and that this implies a reasonable effort to minimize.[94] The mere fact that many innocent conversations were intercepted does not ipso facto vitiate a wiretap.[95]

---

[93] *See, e.g.*, United States v. Scott, 516 F.2d 751, 758 (D.C. Cir. 1975); United States v. Bynum, 360 F. Supp. 400, 412-13 (S.D.N.Y. 1973).

[94] 360 F. Supp. at 409-10; United States v. Armocida, 515 F.2d 29, 42-43 (3d Cir. 1975).

[95] *Id.* In United States v. Manfredi, 488 F.2d 588 (2d Cir. 1973), *cert. denied*, 417 U.S. 936 (1974), the court stated:

> [H]ere as in *Bynum*, the conspiracy unveiled was a huge business involving millions of dollars' worth of narcotics, numerous distributors and highly complex, surreptitious telephone calls. . . . We too fail to see how any detailed screening instructions . . . could be devised under these circumstances. Here no claim is made that the Government could have formulated a pattern of innocent calls by which it could have avoided intercepting those.

Id. at 600.

Although it is a good principle that monitoring agents should be given considerable leeway in what they intercept when the subject matter is complex, the Second Circuit went overboard in this case and permitted a classic failure to minimize. Claiming they could not screen out innocent calls, agents intercepted every single conversation in its entirety—they failed to minimize out even one of 1,595 calls. *Id.* at 599. The court concedes that not even the monitoring agents at the time of interception thought that all the conversations were pertinent, and then admits that the court's own analysis of the transcripts shows that even fewer conversations were relevant. *Id.* at 599-600. Nevertheless, the court concluded: "[W]e believe that the Government made a prima facie showing of compliance with the minimization provision . . . ." *Id.* at 600.

The assertion that the agents were unable to screen out a single conversation despite a good faith minimization effort strains credulity. Only two months after *Manfredi*, in an extremely similar fact situation, the Second Circuit faced a case in which the agents were able to minimize out a meaningful number of privileged and nonpertinent calls. United States v. Rizzo, 491 F.2d 215, 217 (2d Cir.), *cert. denied*, 416 U.S. 990 (1974). The *Rizzo* court, which included two of the same judges that decided *Manfredi*, approved the successful minimization effort with no reference to their permissive opinion in *Manfredi*. Furthermore, in *Bynum*, upon which the court in *Manfredi* relied, agents managed to screen out ten percent of the calls, whereas the *Manfredi* agents failed completely. The only explanation for the puzzling result in *Manfredi* is that the Second Circuit was simply unwilling to suppress evidence and risk letting obviously guilty defendants go free, particularly when they had been in the destructive business of selling millions of dollars' worth of narcotics.

A wrongly-decided opinion like *Manfredi* can have far-reaching and damaging results. Citing the Second Circuit's *Manfredi* opinion, the Seventh Circuit recently permitted agents in one case to intercept every conversation, even though only 153 out of more than 2,000 calls were pertinent. United States v. Quintana, 508 F.2d 867, 873 (7th Cir. 1975). Although the suspects occasionally spoke in colloquial Spanish and used code to confuse the monitors, it is nevertheless hard to believe that the agents were unable to identify a single conversation

Where conversations involving the subject matter under investigation are easily distinguishable from other calls, as in gambling investigations, the courts have allowed fewer interceptions of innocent calls. Gambling is easy to recognize because callers placing bets must specify an event, their choice, and the amount, and this type of conversation cannot be veiled in ambiguous references or code words.[96] Since it is difficult to defend a failure to distinguish between a betting conversation and all others, the courts have allowed fewer interceptions of innocent conversations in gambling investigations than in narcotics investigations.[97]

(4) Use of code. Closely related to the last variable, the use of code or guarded language usually affects a court's willingness to permit interception of innocent conversations.[98] The monitoring agent, making a reasonable effort to distinguish between innocent and evidentiary conversations, may nevertheless be unable to tell the difference and consequently may be forced to intercept nearly all conversations until the code is broken or the agent begins to understand ambiguous guarded language.[99] If the judge is convinced that the agents have made a reasonable effort to make

as nonpertinent. *See also* United States v. Scott, 516 F.2d 751, 753-54, 757 n.13 (D.C. Cir. 1975). The *Quintana-Manfredi* interpretations of minimization could, if not limited or overruled, effectively nullify the statute and raise serious doubts about the viability of minimization.

[96] *See, e.g.*, United States v. Sklaroff, 323 F. Supp. 296, 317 (S.D. Fla. 1971), *aff'd*, 506 F.2d 837 (5th Cir. 1975). *See generally* A.B.A. MINIMUM STANDARDS 31-33.

[97] *Cf.* United States v. George, 465 F.2d 772, 774 (6th Cir. 1972) (failure to minimize in a gambling investigation when suspect was using a public telephone).

[98] *See* United States v. Manfredi, 488 F.2d 588, 593-94, 597 (2d Cir. 1973); United States v. Bynum, 360 F. Supp. 400, 412-13 (S.D.N.Y. 1973).

[99] It is difficult to believe how ambiguous and vague conversations can be until one reads transcripts of actual wiretaps. A good example of the use of code and guarded language is cited in a footnote to United States v. Bynum, 360 F. Supp. 400, 412 n.10 (S.D.N.Y. 1973). The court explained that seemingly innocent conversations were actually codes relating to Bynum's narcotics trade:

> [T]he inspectors detected that word codes and guarded language were employed by the speakers to hide the true meaning of conversations. It was suspected that the codes adopted related to items sold in Bynum's other business enterprises, for example, his clothing store, although other codes were sensed as well. Calls that may on their face have appeared innocent were accordingly monitored; and as the investigation proceeded, the intended meaning of earlier calls dawned on the agents.

Id. at 412-13 (footnote omitted). *See also* United States v. Focarile, 340 F. Supp. 1033, 1048-50 (D. Md.), *aff'd on other grounds sub nom.* United States v. Giordano, 469 F.2d 522 (4th Cir. 1972), *aff'd*, 416 U.S. 505 (1974) (100 percent interception for 12 days was not unreasonable where it was extremely difficult, if not impossible, to determine which calls were innocent until a reliable pattern could be developed); United States v. Capra, 501 F.2d 267, 273-74 (2d Cir. 1974), *cert. denied*, 420 U.S. 990 (1975) (detailing problems agents face when they monitor coded and confusing conversations).

the distinction, the court will not find a failure to minimize.[100] Thus the Second Circuit allowed interception of 100 percent of the calls in *United States v. Manfredi,*[101] where the suspects used a "narcotics code"[102] and where "some seemingly innocuous calls were in fact related to the drug conspiracy."[103] The court failed to see "how any detailed screening instructions which could effectively minimize licit telephone interceptions could be devised under these circumstances."[104]

(5) Length of time tap has run. Since the monitoring agents frequently need time to discern a pattern of conversations to discover which kinds of calls provide evidence and which kinds are innocent, the courts have excused failures to minimize if the failure occurred near the beginning of the tap and was later corrected. A conscientious investigator supervising a tap typically consults with the monitoring agents on a daily basis and, as soon as he can, formulates rules for screening out innocent conversations.[105] But the formulation of patterns and rules may take some time and a court may be willing to excuse transgressions if the agents can show that they were trying to formulate a minimization plan.[106]

---

[100] *See* United States v. Bynum, 360 F. Supp. 400, 410 (S.D.N.Y. 1973).

[101] 488 F.2d 588, 592-93 (2d Cir. 1973), *cert. denied,* 417 U.S. 936 (1974). For a discussion of this case, see note 95 *supra.*

[102] *Id.* at 597.

[103] *Id.* at 600.

[104] *Id. See* United States v. Cox, 462 F.2d 1293, 1300-01 (8th Cir. 1972), *cert. denied,* 417 U.S. 918 (1974). *But see* United States v. Sisca, 361 F. Supp. 735, 744-45 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1008 (1974) (failure to minimize even though code and guarded language was used, and many apparently innocent conversations later were found to be pertinent to the investigation).

[105] In United States v. Falcone, 364 F. Supp. 877 (D.N.J. 1973), the agent in charge formulated minimization rules on the fourth or fifth day of the wiretap (the testimony is unclear on the date). The court explained:

> He placed a card on the recorder with instructions to the monitoring agents not to intercept "Tony's wife Helen" or "Pat's wife Edith" and, on [the seventh day of the wiretap] placed two large charts on the wall of the intercept site instructing the monitoring agents . . . on what were considered privileged conversations, and who was not to be intercepted. . . . Instructions . . . were modified from time to time as the investigation continued.

Id. at 880-81.

[106] Although most or all of the calls in the first few days of the *Falcone* tap presumably were intercepted, the judge found that the agent in charge had properly minimized:

> Under skilled and severe cross examination, confronted by defense counsel with carefully selected conversations, he readily conceded that on occasion monitoring agents had not properly minimized a call. Overall, his testimony reflects a good faith effort on the part of the agents to minimize non-pertinent . . . conversations.

Id. at 881. In United States v. Focarile, 340 F. Supp. 1033, 1048-50 (D. Md. 1972), the court allowed agents investigating a large narcotics conspiracy to intercept all calls for more than twelve days when the supervising attorney thereafter formulated a set of minimization rules. After the initial period of continuous interception, the attorney in charge had determined

(6) Extent of judicial supervision. Where the judge who approved the original eavesdropping order plays an active role in the effort to minimize, other courts passing on the minimization issue in the same case will give considerable deference to the original judge's participation. In *United States v. Bynum*[107] the judge who issued the order and then worked actively with the investigators in the case actually testified at the minimization hearing. Commenting on that testimony, the court wrote: "Where as here it can be found that the Judge carefully and actively supervised the surveillance, his determination that minimization was achieved 'is itself a substantial factor tending to uphold the validity' of that decision."[108] But in *United States v. Sisca,*[109] the court had no trouble finding a failure to minimize when neither the responsible investigators nor the authorizing judge made any effort to devise a plan to screen out innocent conversations.[110]

2. *Special Situations*

There are a number of types of conversations which are protected from interception by special immunities derived from the Constitution and from the common law. Some conversations are protected by legally recognized privileges, and others are protected by the sixth amendment's right to counsel clause.

Analysis of privileges follows the same general two-step

---

that calls to ten numbers were not pertinent, and that all pertinent calls to women turned immediately to talk of narcotics or gambling. *Id.* at 1048. The monitoring agents were therefore instructed not to intercept calls to the ten numbers or calls to women when the conversation did not become immediately pertinent, and the court found that this was an adequate effort at minimization. *Id.* at 1050. *See also* United States v. Scott, 516 F.2d 751, 755 (D.C. Cir. 1975).

[107] 360 F. Supp. 400 (S.D.N.Y.), *aff'd,* 485 F.2d 490 (2d Cir. 1973), *vacated on other grounds,* 417 U.S. 903 (1974).

[108] *Id.* at 414-15, *quoting* United States v. Becker, 334 F. Supp. 546, 549 (S.D.N.Y. 1971), *aff'd,* 461 F.2d 230 (2d Cir. 1972).

[109] 361 F. Supp. 735 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1008 (1974).

[110] The court found a failure to minimize even though 90 percent of the calls later appeared to be pertinent. *Id.* at 743, 745. *But see* United States v. Scott, 516 F.2d 751 (D.C. Cir. 1975), where the court declined to suppress when the agents failed to make any minimization efforts, because the court found that 100 percent interception would have been reasonable even if the agents had attempted to minimize. The court stated:

> [T]he agents could publicly declare their intent to disobey the minimization provisions of the wiretap order, and yet it is possible that the ultimate interceptions will be found to have been reasonable. . . . [T]he decision on the suppression motion must ultimately be based on the reasonableness of the actual interceptions and not on whether the agents subjectively intended to minimize their interceptions.

Id. at 756.

process used with pertinent and nonpertinent conversations. What conversations are privileged and therefore cannot be used in evidence? What happens if one or more privileged conversations are intercepted?

Although conversations between husband and wife, doctor and patient, priest and penitent, and lawyer and client have all traditionally been shielded by an evidentiary privilege,[111] the lawyer-client situation has appeared most often in the wiretap cases. This type of conversation is also the most heavily guarded by legal protections, since the due process and right to counsel clauses of the fifth and sixth amendments have been construed to protect the confidentiality of the lawyer-client relationship in certain situations.[112]

Not every conversation between lawyer and client is protected, however. The privilege exists for the benefit of the client only, and the lawyer may not claim protection when his incriminating conversations are intercepted.[113] Furthermore, only conversations

[111] *See generally* 8 J. WIGMORE, A TREATISE ON THE ANGLO-AMERICAN SYSTEM OF EVIDENCE (McNaughton rev. 1961) §§ 2290, 2291, 2298, 2310, 2321, 2326 (attorney-client); §§ 2227, 2228, 2232, 2233, 2236-39, 2241 (husband-wife); §§ 2380-2391 (doctor-patient); §§ 840, 2394 (priest-penitent); FED. R. EV. 503-06 (1975). *Cf.* A.B.A. MINIMUM STANDARDS 152-58.

While the privileges have traditionally allowed one party to a privileged communication to prevent the other party from testifying in court to the contents of the communication, the addition of the wiretapping factor added a third party—the eavesdropper. The first courts to rule on the application of the privilege against eavesdropping third parties held that the eavesdropper was free to testify to what he had overheard, because the communication lost its privileged character when it was intercepted. *See* Commonwealth v. Wakelin, 230 Mass. 567, 120 N.E. 209 (1918); Clark v. State, 159 Tex. Crim. 187, 261 S.W.2d 339, *cert. denied,* 346 U.S. 855 (1953).

This rule, formulated when eavesdropping was infrequent, would have serious consequences if it were applied in the thousands of present day wiretaps. Clients would be afraid to speak freely to their lawyers, for instance, for fear that a statement would be overheard and used against them. The draftsmen of Title III, specifically recognizing this problem, included 18 U.S.C. § 2517(4) (1970), which provides: "No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." *Id.* This section reversed the rule of *Wakelin* and preserves the privacy of communications that are entitled to a privilege.

> The Department of Justice explains to its attorneys in its in-house wiretap manual: [T]he confidentiality of conversations between individuals who stand in the relationship of husband-wife, clergyman-penitent, physician-patient, and attorney-client are protected by testimonial privilege. If a defendant could properly assert such a privilege against introduction of his conversations when the Government had obtained evidence of them through normal investigative techniques, then it was not the intent of Congress to allow the Government to use these conversations as evidence when obtained through electronic surveillance.

JUSTICE DEPT. MANUAL 35.

[112] *See generally* Note, *Government Interceptions of Attorney-Client Communications,* 49 N.Y.U.L. REV. 87 (1974).

[113] United States v. King, 335 F. Supp. 523, 545-46 (S.D. Cal. 1971), *rev'd on other grounds,* 478 F.2d 494 (9th Cir. 1973), *cert. denied,* 417 U.S. 920 (1974).

that relate to a professional association fall under the privilege—neither party to the conversation may claim a privilege for a conversation that relates to ongoing criminal activities where the lawyer is not acting in his professional capacity.[114]

If the reported cases are a good sample, it appears that in most wiretaps in recent years the monitoring agents have been routinely instructed not to intercept privileged conversations.[115] Inevitably, however, some of these conversations occasionally find their way into the agents' tapes, and the courts have consistently refused to find a failure to minimize.[116] As long as a serious effort is made to screen out privileged calls, the court will not suppress because the effort was not completely successful.[117]

The marital privilege has been treated in similar fashion. In one case the Seventh Circuit reasoned that the public interest in discovering the truth about crime outweighed any social interest in marital privacy.[118] Although the court would recognize the privilege as to innocent husband-wife conversations, it would not suppress conversations that "had to do with the commission of a crime"[119] or that "were with respect to ongoing violations of Illinois gambling laws."[120] The marital privilege has thus been interpreted to shield from interception little that would not be otherwise protected under the minimization section. Husband-wife conversations are shielded only to the extent that the conversation legitimately falls within the intimacy of the marital relationship; in other words, almost anything incriminating can be intercepted, and if it is protected by the marital privilege, the conversation is irrelevant and the prosecution would not want to use it anyway. The doctor-patient and priest-penitent privileges apparently have

[114] *Id.* In United States v. Bynum, 360 F. Supp. 400 (S.D.N.Y. 1973), the court stated: "A call from a lawyer to a person is not automatically privileged . . . . The attorney-client privilege exists where the purpose of the communication is to obtain professional legal advice . . . not news of others, gossip or criminality." *Id.* at 417.

[115] *See, e.g.*, United States v. Bynum, 360 F. Supp. 400, 406 (S.D.N.Y. 1973); United States v. LaGorga, 336 F. Supp. 190, 195 (W.D. Pa. 1971); United States v. Sklaroff, 323 F. Supp. 296, 317 (S.D. Fla. 1971), *aff'd*, 506 F.2d 837 (5th Cir. 1975).

[116] United States v. Falcone, 364 F. Supp. 877, 885 (D.N.J. 1973); United States v. Bynum, 360 F. Supp. 400, 418 (S.D.N.Y. 1973).

[117] In *Falcone* the court held that the monitoring agents had done an adequate job of minimization even though agents did not shut off their machines on two calls to a lawyer: "There were six calls between Del Vecchio and his lawyer's office. Four were minimized in less than one minute. The two which were not minimized lasted, respectively, one minute, and 40 seconds." 364 F. Supp. at 885.

[118] United States v. Kahn, 471 F.2d 191 (7th Cir. 1972), *rev'd on other grounds*, 415 U.S. 143 (1974).

[119] *Id.* at 194.

[120] *Id.* at 195. *See also* Note, *The Future Crime or Tort Exception to Communications Privileges*, 77 HARV. L. REV. 730, 734 (1964); Annot., 4 A.L.R.2d 835 (1948).

not yet been litigated in the wiretapping context, although one court noted, in ruling that agents had failed to minimize, that many intercepted calls to doctors could easily have been privileged.[121]

The sixth amendment's guarantee of assistance of counsel is now interpreted to apply at all critical stages of the prosecution.[122] Most post-indictment encounters with the police have been held to be critical stages, and the defendant is entitled to have counsel present.[123] If an indicted defendant divulges incriminating information to a police informant in the absence of counsel while the police secretly listen through the use of a wiretap, the information so obtained is probably in violation of the defendant's sixth amendment rights,[124] is suppressible,[125] and may taint other evidence obtained through direct use of the wiretap.[126] Conversations between an indicted person and his attorney are absolutely protected by the fifth and sixth amendments, and the mere interception of such conversations may result in a mistrial.[127] Although the indicted person situation has not yet come up in Title

[121] United States v. Sisca, 361 F. Supp. 735, 744 (S.D.N.Y. 1973).

[122] Simmons v. United States, 390 U.S. 377, 382-83 (1968).

[123] *See* United States v. Wade, 388 U.S. 218 (1967); Gilbert v. California, 388 U.S. 263 (1967); Massiah v. United States, 377 U.S. 201 (1964).

[124] Massiah v. United States, 377 U.S. 201 (1964). The precise holding of *Massiah* is confined to the situation in which the police elicit incriminating statements from an indicted person in the absence of counsel. The police had used a radio transmitter to listen in on a conversation between the indicted defendant and a former associate who had, unknown to Massiah, decided to cooperate with the authorities. The Court held that this procedure was an interrogation and that use of the information in evidence would violate the defendant's sixth amendment right to effective assistance of counsel. *Id.* at 206. Use of a police informant to entice an indicted defendant into making incriminating statements on a wiretapped line would thus be prohibited by *Massiah.* This holding might arguably be extended to prohibit interception of a conversation between an indicted person and an informant, even if the conversation were fortuitous and the informant did not attempt to elicit incriminating information.

[125] Mapp v. Ohio, 367 U.S. 643 (1961); Weeks v. United States, 232 U.S. 383 (1914).

[126] Wong Sun v. United States, 371 U.S. 471 (1963).

[127] Caldwell v. United States, 205 F.2d 879, 881 (D.C. Cir. 1953), *cert. denied,* 349 U.S. 930 (1955) (use of informant); Coplon v. United States, 191 F.2d 749, 757, 759 (D.C. Cir. 1951), *cert. denied,* 342 U.S. 926 (1952) (use of wiretap). *See* State v. Cory, 62 Wash. 2d 371, 382 P.2d 1019 (1963) (presumption that surveillance of attorney-defendant relationship constitutes an intrusion on constitutional rights; conviction reversed and further prosecution prohibited). *But see* United States v. Lebron, 222 F.2d 531, 535 (2d Cir.), *cert. denied,* 350 U.S. 876 (1955) (no presumption that surveillance is an unconstitutional intrusion on the defense). *See also* A.B.A. MINIMUM STANDARDS 154-56.

The Department of Justice instructs its supervising attorneys:

> In the event that the electronic surveillance intercepts a communication between an attorney and client concerning a *pending* criminal case, that is, a case in which the client is under indictment, the agent supervising the interception must immediately shut off the interception equipment and make a notation in the logs that the conversation was shut off and was not overheard.

JUSTICE DEPT. MANUAL 37 (emphasis in original).

III litigation, it seems clear that monitoring officers must be unusually careful when they overhear indicted defendants' conversations.[128]

C. *Techniques*

Once it is decided which conversations may not be intercepted, the monitoring agents must determine as a practical matter how best to avoid intercepting them. There are basically two methods available by which to limit interceptions: extrinsic minimization, which entails intercepting only at specified times, and intrinsic minimization, which entails determining the content of calls as they are intercepted, and making an on-the-spot decision as to whether to continue monitoring them.

Extrinsic minimization can be highly effective if the purpose of the wiretap is to develop incriminating evidence against one or more known individuals and if the monitoring agents can maintain visual surveillance of the telephone being tapped. It is then a simple matter for the surveillance agent to inform the interception station that one of the suspects has picked up the receiver.[129] Intrinsic minimization can then be applied, and the result is likely to be an extremely precise series of interceptions with very little overage.

The extrinsic method is not useful, however, if the suspects are not identified, so that visual surveillance is not helpful, or if visual surveillance is not possible. The only extrinsic method left would then be to restrict interception to certain hours of the day.[130]

---

[128] *See* note 124 *supra.* A clever criminal who fears he is being wiretapped could create problems for the monitors and grounds for appeal in the future by calling his indicted friends daily and consulting frequently with his lawyer.

[129] In Katz v. United States, 389 U.S. 347 (1967), the Supreme Court approved of just such a method of minimization, even though the wiretap was held invalid for failure to procure a warrant. The Court stated: "The agents confined their surveillance to the brief periods during which he used the telephone booth, and they took great care to overhear only the conversations of the petitioner himself." *Id.* at 354. In a footnote to the opinion the Court added: "Based upon their previous visual observations of the petitioner, the agents correctly predicted that he would use the telephone booth for several minutes at approximately the same time each morning. The petitioner was subjected to electronic surveillance only during this predetermined period." 389 U.S. at 354 n.14. *See also* United States v. Sklaroff, 323 F. Supp. 296, 317 (S.D. Fla. 1971), *aff'd,* 506 F.2d 837 (5th Cir. 1975) (extrinsic minimization applied successfully). *But see* United States v. George, 465 F.2d 772, 774 (6th Cir. 1972) (failure to apply extrinsic minimization to a public telephone booth).

[130] *See* State v. Dye, 60 N.J. 518, 527, 291 A.2d 825, 829, *cert. denied,* 409 U.S. 1090 (1972). This technique is of some use when relevant calls are expected to be concentrated within known hours, or if experience with the individual wiretap shows that certain hours are productive and others are not. In most cases, however, pertinent calls are made at all hours of the day; no times can be singled out as more or less productive; no visual

Curiously enough, the State of New Jersey, which operates under a statute containing minimization language more restrictive than the language in Title III,[131] chose the extrinsic method as a rule of law in *State v. Dye*.[132] Explaining that the monitors can never determine when an innocent conversation will turn to incriminating matters, the court effectively ruled that the monitor need not ever turn his machine off during the hours prescribed for interception.[133] The court apparently believed that transcribing only the guilty conversations is an adequate protection against invasion of privacy.[134]

It is difficult to reconcile this approach with the New Jersey statute, which closely follows Title III. Under the extrinsic approach, the monitoring agent can listen to and record the conversations of hundreds of innocent patrons of a public telephone, if visual surveillance is impractical, while he waits for the suspect to use the booth. This was the case in *Dye*.[135] Those innocent people would never be identified, never notified, and would never know that the police had intercepted their calls.[136]

---

surveillance is possible; and extrinsic minimization is impossible. *See, e.g.*, United States v. James, 494 F.2d 1007 (D.C. Cir.), *cert. denied*, 419 U.S. 1020 (1974), where "calls came in during all hours of the day and night at the rate of one every ten minutes." *Id.* at 1022.

[131] N.J. STAT. ANN. § 2A:156A-12(f) (1971) uses the words "minimize or eliminate" while the federal statute uses only the word "minimize." 18 U.S.C. § 2518(5) (1970).

[132] 60 N.J. 518, 291 A.2d 825, *cert. denied*, 409 U.S. 1090 (1972). Prior to *Dye*, a New Jersey lower court had written a comprehensive minimization opinion that adopted the intrinsic method. State v. Molinaro, 117 N.J. Super. 276, 284 A.2d 385 (1971). This decision was reversed in light of *Dye*, 122 N.J. Super. 181, 299 A.2d 750, *cert. denied*, 62 N.J. 574 (1973), and the New Jersey rule is now clearly extrinsic. The New Jersey legislature has recently incorporated the *Dye* holding into its wiretap authorization statute:

> Every order . . . shall require that . . . interception . . . be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this act by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order.

N.J. STAT. ANN. § 2A:156A-12(f) (amended June 30, 1975). For a brief explanation of the amendment, see NEW JERSEY ATTORNEY GENERAL, REPORT ON THE NEW JERSEY WIRETAPPING AND ELECTRONIC SURVEILLANCE CONTROL ACT 22-24.

Although the amended statute encourages extrinsic minimization, it seems clear that individual prosecutors are free to employ intrinsic methods as well. The Essex County prosecutor, for instance, "requires his monitors to turn off the tap when nonpertinent telephone calls are being intercepted." HEARINGS BEFORE THE NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE, *Staff Report on Essex County*, Tab J, at 4 (March 18-20, 1975).

[133] 60 N.J. at 538-39, 291 A.2d at 835.

[134] *Id.* at 536-37, 291 A.2d at 834.

[135] *Id.* at 523-25, 291 A.2d at 827-28.

[136] Justice Douglas, dissenting in the denial of the petition for certiorari, agreed:

> Although the authorization order limited the conversations to be seized, the execution of the order included seizure of all conversations on the telephone over the period of the wiretap. Such an invasion of privacy is even more horrendous

The federal courts have spurned the New Jersey approach and have adopted the intrinsic method as their rule,[137] supplemented where possible by extrinsic methods. The federal system is therefore generally more effective in safeguarding privacy. Instead of blindly intercepting all conversations within a given time period, a carefully administered and conscientiously applied program of intrinsic minimization can screen out most truly private conversations.[138]

Where the intrinsic method is used, agents typically listen carefully to the first minute or so of the call, and then shut off their equipment if they determine it is not pertinent.[139] The agents may periodically sample the content of longer calls to make certain that neither the parties nor the subject matter has changed.[140] If agents frequently switch the recorders on and off as conversations take pertinent and nonpertinent turns, however, the taped record produced will be marked by gaps and jumps. This is clearly a serious problem, since the statute directs that the recording "be

> since it involves a pay telephone in a public place where the majority of users and conversations, as indicated by the 102½ hours of innocent conversations out of the 105 hours of seized conversations, will have no relationship to the alleged criminal activity. . . . [T]he authorization of the wiretap in the instant case . . . is the equivalent of a general warrant.

409 U.S. 1090, 1092-93 (1972). The New Jersey statute has recently been amended to incorporate the holding of *Dye*. See note 132 *supra*.

[137] *See, e.g.*, United States v. Askins, 351 F. Supp. 408, 415 (D. Md. 1972). In addition, the Supreme Judicial Court of Massachusetts recently interpreted its wiretap statute to require intrinsic minimization. Commonwealth v. Vitello, 327 N.E.2d 819, 844 (Mass. 1975).

[138] *See, e.g.*, United States v. Curreri, 363 F. Supp. 430 (D. Md.), *supplemented*, 368 F. Supp. 757 (D. Md. 1973). Out of 2361 calls intercepted, the prosecution and defense stipulated that 899 were pertinent and properly intercepted, and 1043 were properly terminated by the agents. The defendants, however, claimed that 419 more should have been terminated or terminated sooner. The judge ruled that minimization had been properly achieved, pointing out that many of the defendants' 419 calls were in fact terminated at some point, that most involved one of the defendants, and that many were very short and could not have been shut off before the call ended. The government clearly made a good-faith effort here to comply with the minimization directive, and was evidently successful in screening out a high percentage of calls. 363 F. Supp. at 436.

[139] *See id.* at 436-37; United States v. Falcone, 364 F. Supp. 877, 880 (D.N.J. 1973).

[140] United States v. Bynum, 360 F. Supp. 400, 413 (S.D.N.Y. 1973). Sampling is necessary to thwart wary criminals who slip a few incriminating statements into a long, chatty, personal call. The classic example of this kind of call occurred in the investigation which led to United States v. King, 335 F. Supp. 523 (S.D. Cal. 1971), and which is universally quoted. The court cited a conversation which had been intercepted in its entirety, and which ran for 45 pages of transcript. The conversation was completely irrelevant, except for two pages right in the middle where the conversation "turned briefly but pointedly to the conspiracy." 335 F. Supp. at 541. Although the court in *King* used this conversation as an example of something which should not have been intercepted, other courts have mistakenly cited this example to support a contention that nearly everything should be intercepted because relevant material can appear at any moment. One such case is State v. Dye, 60 N.J. 518, 538, 291 A. 2d 825, 835, *cert. denied*, 409 U.S. 1090 (1972). For a discussion of this case, see notes 132-36 and accompanying text *supra*.

done in such a way as will protect the recording from editing or other alterations."[141] Even if the recording was not actually altered or edited, and the government can show that this is true, a defendant could always charge that the recording was not made in such a way as would protect against alterations.[142] It would therefore appear desirable to have a complete tape, which would be available only to the judge and to the defendants, for the purpose of having an edit-proof system. It would not be difficult to use a voice-actuated recorder, with no playback device and enough tape to last eight or twelve hours, in addition to the agent's regular working recorder, in order to produce the complete tape.[143]

Although recording all conversations would seem to be a violation of minimization in itself, there is no reason, as noted above, why the definition of interception cannot exclude court-supervised recordings which are unavailable to the police or prosecution and which are undertaken solely for the benefit of the defendants.[144]

D. *Remedies*

Title III provides a suppression remedy that applies to the contents of any "communication" which was "unlawfully

[141] 18 U.S.C. § 2518(8)(a) (1970).

[142] *Cf.* United States v. Leta, 332 F. Supp. 1357 (M.D. Pa. 1971). The court said in dicta: "Furthermore, nearly continuous seizure . . . of the defendant's phone conversations may protect the defendant from having these conversations edited to his detriment or having statements taken out of context." 332 F. Supp. at 1360.

[143] Agents frequently make use of a second recorder anyway. The use of additional machines should not be a significant financial drain, therefore, and no extra manpower would be needed, since the machine would be unattended and would work with no human assistance except when tapes have to be changed. Voice-actuated recorders are already in common use to avoid wasting tape and to relieve the agents of the necessity of switching on and off for each call. The agents could always play back the tape thus produced before it was taken away and sealed, but if this problem proves to be serious in practice the recorder could be placed in an isolated location to which the agents have no access, or it could be sealed shut, and the tapes changed and removed by a court-appointed representative. The Nassau County, New York District Attorney's office has confirmed that it uses this dual-tape method in all its wiretaps.

[144] *See* text accompanying note 65 *supra*. Although the dual-tape method solves the editing problem, it also raises several other problems. First, agents who find that they mistakenly minimized an important conversation will certainly apply for a search warrant to listen to that conversation on the master tape. The warrant should issue upon a showing of probable cause that a particular conversation will yield evidence, but only if the agents can show that they can locate the desired conversation without listening to excessive portions of the master tape. Complete recording is an evil that should be tolerated only to protect the defendant from editing, and the government should not be allowed to turn this procedure to its own advantage by listening freely to long sections of the master tape. Second, if a court rules that use of a nonminimized master tape is a violation of minimization, what is to be suppressed? Clearly, only the nonminimized tape should be suppressed; the properly minimized tape is lawfully and independently produced, and so is not a "fruit" of the illegality.

intercepted" or which was intercepted "not . . . in conformity with the order of authorization."[145] While this language clearly gives the defendant a right to suppress evidence when there was a failure to minimize, it is not at all clear how much evidence Congress intended to be suppressed. A court could either suppress all evidence arising from a wiretap that produced excessive overage, or it could suppress only the overage, leaving the pertinent conversations free to be used in evidence.

The first two cases to consider the question split evenly, one choosing total suppression, the other deciding on suppression only for improperly intercepted conversations. In *United States v. Scott*[146] the court suppressed all evidence when it found a failure to minimize. A later case[147] that followed *Scott* reasoned that if only improperly intercepted conversations were suppressed, investigators would be free to intercept every conversation in every case, since they would know that a court would not suppress the incriminating conversations—the very ones the prosecution would introduce into evidence.[148] Therefore, the court applied total suppression as a more potent weapon.[149]

Taking a more statutory and historical perspective, the court in *United States v. King*[150] decided to suppress only conversations that were improperly intercepted.[151] Previously, the court reasoned, all evidence obtained from a search and seizure was to be suppressed only if the search was void *ab initio,* and that was not the case with a valid warrant that had been improperly executed.[152] When officers executing a valid warrant go beyond the scope of permissible seizure, the validly seized items are not tainted and may be introduced in evidence. The invalidly seized items, however, are suppressed and in the usual case are returned to their owner.[153]

---

[145] 18 U.S.C. § 2518(10)(a) (1970).

[146] 331 F. Supp. 233 (D.D.C. 1971), *vacated,* 504 F.2d 194 (D.C. Cir. 1974). On remand, the district court again ordered suppression, but the court of appeals reversed, 516 F.2d 751 (1975), holding that there had been no failure to minimize and that total suppression was not the proper remedy in any event.

[147] United States v. Focarile, 340 F. Supp. 1033 (D. Md. 1972).

[148] *Id.* at 1046-47. Courts usually rule that incriminating conversations were properly intercepted, so the only conversations improperly intercepted, frequently, are the nonpertinent, innocent conversations. *See* text accompanying note 163 *infra.*

[149] *Id.* at 1047.

[150] 335 F. Supp. 523 (S.D. Cal. 1971), *rev'd on other grounds,* 478 F.2d 494 (9th Cir. 1973), *cert. denied,* 417 U.S. 920 (1974).

[151] *Id.* at 543-44.

[152] *Id.* at 544.

[153] *Id. See also* United States v. Sisca, 361 F. Supp. 735, 745-46 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1006 (1974); United States v. LaGorga, 336 F. Supp. 190, 196-97 (W.D. Pa. 1971); United States v. Leta, 332 F. Supp. 1357, 1360 (M.D. Pa. 1971);

The court in *King* found further support for its position by reference to the language of Title III.[154] The statute provides that "any . . . communication" may be suppressed,[155] implying that each communication is to be treated individually and that the draftsmen of the statute never intended the suppression remedy to apply in blanket fashion to all communications.[156]

In fact, the statute is ambiguous, and judging from the otherwise precise nature of Title III, Congress would doubtless have specified the intended scope of suppression had it really had any intentions. For the second time[157] the courts have encountered a wiretap situation where there is no real statutory guidance and where search and seizure precedent is misleading because of the differences between wiretapping and the traditional search for tangible evidence.[158] Perhaps in unwritten recognition of this problem, the courts have generally applied a practical rule which combines both partial and total suppression.

Failures to minimize may be divided into two different categories. In the first the investigators make no effort to minimize, and every or virtually every conversation is intercepted.[159] In the second, some effort to minimize is made, but the court rules that the effort is unsatisfactory and that too many nonpertinent conversations were intercepted.[160]

Total suppression has generally been reserved for cases of total failure to minimize, and partial suppression has been applied more often to situations where the minimization effort was made, but was unsatisfactory.[161] A rule combining both types of

United States v. Escandar, 319 F. Supp. 295, 300-01 (S.D. Fla. 1970), *rev'd on other grounds sub nom.* United States v. Robinson, 468 F.2d 189 (5th Cir. 1972).

[154] 335 F. Supp. at 545.

[155] 18 U.S.C. § 2518(10)(a) (1970).

[156] 335 F. Supp. at 545.

[157] *See* notes 35-42 and accompanying text *supra.*

[158] *See* notes 43-54 and accompanying text *supra.*

[159] *See, e.g.,* United States v. George, 465 F.2d 772 (6th Cir. 1972); United States v. Scott, 331 F. Supp. 233 (D.D.C. 1971), *vacated,* 504 F.2d 194 (D.C. Cir. 1974). For the subsequent history of *Scott,* see note 146 *supra.*

[160] *See, e.g.,* United States v. LaGorga, 336 F. Supp. 190, 195-97 (W.D. Pa. 1971).

[161] *LaGorga, George* and numerous other cases would fit under this analysis. *See* notes 159-60 and accompanying text *supra. But see* United States v. Sisca, 361 F. Supp. 735, 744-46 (S.D.N.Y. 1973), *aff'd,* 503 F.2d 1337 (2d Cir.), *cert. denied,* 419 U.S. 1008 (1974) (total failure to minimize, but partial suppression applied). As the government became aware of the penalty for a total failure to minimize, these total failure cases faded away and now some effort at minimization is nearly always made. The total suppression remedy is therefore rarely used in the most recent cases. In fact, judicial findings of failure to minimize have also grown infrequent in the most recent cases as minimization techniques have become more sophisticated.

suppression remedy makes a great deal of sense since it applies graduated penalties to different degrees of infraction. The partial suppression component, however, is dangerously close to no remedy at all, and the trial court must apply it diligently if it is to have any effect.[162] If partial suppression is adopted, the evidence to be suppressed should be that which is derived from improperly intercepted conversations. Before each conversation is received in evidence, then, the defense must be allowed to object to it on the ground that it was improperly intercepted.[163]

In addition to suppression, Title III provides for a civil remedy for anyone whose wire or oral communications are illegally intercepted, used, or disclosed.[164] Any person committing such an infraction will be liable for actual damages, punitive damages, and attorney's fees. Actual damages are set at a minimum of $100 per day or $1,000, whichever is higher. However, good faith reliance on a court order is specified to be a complete defense to an action brought under this section.

Each time a judge rules that there has been a failure to minimize, the possibility arises of a civil suit under this section.[165]

[162] If the trial court merely offers to suppress nonpertinent information, then partial suppression will not impede the prosecution, since the government will certainly not offer irrelevant conversations as evidence. What should be a vindication of the defendant's rights, therefore, becomes nothing more than a verbal reproach from the bench.

[163] If the prosecution attempts to introduce a short segment from the middle of a long personal conversation, the defense must be allowed to argue that the monitoring agents should not have been listening to that call at all, and so should never have heard the incriminating segment. The agents would have been permitted to sample the call, of course, so the judge must finally decide whether he thinks that under the circumstances the agents would have overheard the segment if they had been operating lawfully.

[164] 18 U.S.C. § 2520 (1970).

[165] In United States v. Cox, 462 F.2d 1293, 1301 (8th Cir. 1972), *cert. denied,* 417 U.S. 918 (1974), the court stated in dicta that if monitoring agents failed to minimize, the defendants would bave a cause of action against the individual agents under 18 U.S.C. § 2520 (1970). It is clear from the language of the statute that any person whose conversation is improperly intercepted would have such a cause of action, but in reality suits by nondefendants are rarely brought because the people who are unconnected with the conspiracy never know that their communications have been overheard. They are not arrested and indicted; they may never be identified; and even if identified, they are usually not notified that their conversations were intercepted.

Suits by nondefendants against monitoring agents who fail to minimize could become more frequent if the procedure followed by one district court is adopted. The court in United States v. LaGorga, 336 F. Supp. 190, 197 (W.D. Pa. 1971), acting pursuant to a discretionary power of notification granted in 18 U.S.C. § 2518(8)(d) (1970), ordered all persons whose conversations were intercepted to be notified so that they might take advantage of § 2520 if they so chose. Under § 2518(8)(d), all parties named in the eavesdropping order must be notified within 90 days after the termination of the interception that their conversations were or were not intercepted. The judge has discretionary power to order notification of any other persons as justice may require. *See* notes 233-313 and accompanying text *infra.*

Curiously enough, however, the civil litigation has been confined to violations other than failure to minimize.[166] Criminal defendants have not yet made use of the civil remedy, most probably because of the statutory provision that good faith reliance on a court order constitutes a complete defense. All the agents need do is point to some minimization effort, and the court is likely to direct a verdict for the agents on the ground that they acted in good faith and relied upon a court order.

II
AMENDMENTS

A. *New Crime*

Because the subjects of electronic surveillance may engage in several different criminal enterprises simultaneously, it is not unusual for monitoring agents to intercept conversations providing evidence of crimes other than those set out in the warrant. High level figures in organized crime may engage in gambling, drugs, loan-sharking, securities fraud, and other offenses,[167] so that an investigation into any one area predictably yields evidence in others. Recognizing that this phenomenon will occur, the draftsmen of Title III provided that evidence of a new crime[168] may be used at trial "when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter."[169] This section creates a statutory plain view doctrine for wiretaps, legalizing the interception of evidence found within the scope of an otherwise lawful wiretap,[170] but it reaches further than the traditional doctrine of plain view.

---

[166] One salient example is the suit by the Democratic National Committee against the Committee to Reelect the President, arising out of the celebrated Watergate bug. The suit was brought under § 2520 for violations of § 2511, which prohibits private wiretapping. *See* N.Y. Times, June 22, 1972, at 44, col. 1. *See also* Kinoy v. Mitchell, 331 F. Supp. 379 (S.D.N.Y. 1971) (suit against federal officials for illegal surveillance).

[167] *See generally* THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 192-95 (1967).

[168] A new crime is one not specified in the authorization order.

[169] 18 U.S.C. § 2517(5) (1970). Note that the statute conditions admissibility in evidence on making the application, but does not similarly condition the validity of the original interception.

[170] The plain-view doctrine holds that any evidence that is within the plain view of an officer executing an otherwise lawful search may be validly seized, even though the items are not described in the warrant. *See* Cady v. Dombrowski, 413 U.S. 433 (1973); Coolidge v. New Hampshire, 403 U.S. 443 (1971). For a discussion of the application of plain view to the wiretap situation, written before *Coolidge* and *Cady*, see A.B.A. MINIMUM STANDARDS 142-45.

Whereas the traditional search is conducted within a short space of time, the wiretap may extend for months. An officer executing a search for tangible evidence cannot realistically be expected to seek judicial sanction each time he enters a new room of a house and finds evidence not described in the warrant.[171] But a wiretap monitor might be thought to be executing an unreasonable search if he continued, day after day, to intercept evidence of crimes not specified in the authorization order.[172] Because the fourth amendment prohibits unreasonable searches, it may be a constitutional necessity to obtain immediate judicial approval of the widened scope of interception. The amendment question is thus of constitutional dimension when the monitoring officer seeks to continue intercepting evidence of crimes not specified in the warrant.[173]

For this reason Title III commands the monitoring officer to seek judicial sanction for interception of evidence of new crimes "as soon as practicable."[174] Because new crimes appear frequently,

[171] For this reason an officer executing a search for tangible evidence acts pursuant to a single judicial grant of authority contained in the warrant. If the officer sees evidence not described in the warrant, he may seize it without changing the warrant, and the evidence is later admissible in all trials. Changing, or amending, the conventional warrant would be impractical because the search must be conducted within a matter of hours. A wiretap may extend for months, however, and it is not impractical to amend the wiretap order at intervals as the situation may require.

[172] Since it is impractical to amend a conventional warrant, seizure of an item in plain view without prior judicial approval is reasonable and therefore permissible under the fourth amendment. But the plain-view doctrine is only an exception to the usual requirement of probable cause. When the monitoring agent seeks to intercept future conversations yielding evidence of a new crime, there is no reason why he cannot show probable cause and request that the order be amended. Therefore, failure to amend would be unreasonable, and the conversations not covered by the order would be intercepted illegally. *See* note 174 *infra*.

[173] But note that the point is moot if the tap is terminated upon interception of evidence of the new crime; the search is finished, judicial review would be purely retrospective, and, as in the case of a conventional search, it would be unnecessary to amend the warrant.

[174] 18 U.S.C. § 2517(5) (1970). An amendment can serve two distinct functions. First, it can sanction the past interception of a conversation outside the scope of the order. Second, it can provide judicial approval of future interceptions of conversations outside the scope of the order. For the first type of amendment, the judge need only determine that the conversation was properly in plain view; the original order must have been valid and the agents must have conducted the wiretap in a lawful manner. For the second type of amendment, however, the judge is actually granting a new, enlarged authorization order. Therefore, the government must support its application for this *prospective* amendment with a showing of probable cause. The legislative history of § 2517(5) shows clearly that the draftsmen envisioned only the first, retrospective, type of amendment. LEGISLATIVE HISTORY 2189. When there is probable cause to believe that evidentiary conversations outside the scope of the warrant will be intercepted in the future, however, the Constitution requires a prospective amendment supported by a showing of probable cause. People v. Di Stephano, 45 App. Div. 2d 56, 60-61, 356 N.Y.S.2d 316, 320-21 (1st Dep't 1974); People v. Di Lorenzo, 69 Misc. 2d 645, 651, 330 N.Y.S.2d 720,

particularly in investigations of organized crime, and because overworked police officers and prosecutors frequently do not immediately file applications with the judge, a number of courts have had to determine whether a particular amendment was obtained "as soon as practicable," and, if not, whether evidence should be suppressed.

The amendment cases fall into two major categories: first, those cases where surveillance ends substantially at the point where the new crime is perceived, and second, those cases where surveillance continues after perception of the new crime. The first category presents no problems.

1. *Surveillance Terminates*

In *People v. Ruffino*[175] the monitoring officers ended the wiretap shortly after intercepting the first indications of a new crime. Although a post hoc amendment of the warrant after surveillance has terminated might seem pointless from a constitutional viewpoint, the language of the statute requires an amendment every time the government wants to use at trial evidence of a new crime, regardless of the circumstances.[176] The monitoring officers in this case thus should have applied for an amendment immediately, but in fact they delayed for months.[177]

727 (County Ct. 1971). This prospective amendment would be necessary even though Title III does not explicitly provide for such a procedure.

This distinction between the two types of amendment can place investigators in a very difficult position. If they intercept a small number of conversations providing evidence of a new crime, their experience may give them a "hunch" that a crime is being planned and that more such conversations will occur. But a mere hunch does not constitute probable cause and the investigators would be unable to obtain a prospective amendment. At the same time, the defense could argue that the investigators were knowingly intercepting conversations beyond the scope of the order and that the search was therefore unreasonable. The New York Appellate Division accepted this defense in People v. Di Stephano, 45 App. Div. 2d 56, 356 N.Y.S.2d 316 (1st Dep't 1974). The *Di Stephano* result appears to put New York investigators in a hopeless dilemma, and the New York County District Attorney has appealed this case to the New York Court of Appeals. The best answer to the problem is to allow interception of conversations providing evidence of a new crime until the government first accumulates probable cause. Up to this point, the conversations would be in plain view and retrospective amendments would be required. When the judge determines that the conversations amount to probable cause, he should require the government to enlarge the scope of the warrant with a prospective amendment. The prosecutor should not risk suppression simply because he erred in determining the exact point at which he had enough evidence to obtain a prospective amendment.

[175] 62 Misc. 2d 653, 309 N.Y.S.2d 805 (Sup. Ct. 1970).

[176] N.Y. CRIM. PRO. LAW § 700.65(4) (1971). This section is substantially identical to the Title III amendment section, 18 U.S.C. § 2517(5) (1970).

[177] 62 Misc. 2d at 655, 309 N.Y.S.2d at 808.

Nevertheless, despite the "as soon as practicable" language, the court refused to suppress.[178]

Although one purpose of Title III's amendment section[179] is to provide judicial sanction for ongoing interception of communications not specified in the warrant,[180] the legislative history shows that the amendment is also designed to give the judge an opportunity to ensure that the original order was lawfully obtained, was "sought in good faith and not as subterfuge search," and "was in fact incidentally intercepted during the course of a lawfully executed order."[181] Since surveillance in this situation has already ended, there is no need to seek judicial approval for continuing interception of evidence of a new crime, and no constitutional question is involved.[182] The other aims specified in the legislative history are a restatement of the elements of the plain view doctrine: the original order must not have been sought as a subterfuge when the government's real purpose was to obtain evidence of the new crime, and the communications must really be incidentally intercepted while the monitors were looking for something else.

In the termination of surveillance case, therefore, interception has ended and the amendment can only apply retrospectively.[183] Since the amendment only sanctions events in the past, failure to file promptly does not affect the legality of future surveillance and does not affect any of the defendant's rights. Thus, whether the government files the amendment as soon as practicable or not makes no difference. And because neither the legality of the surveillance nor the rights of the defendant turn on the timing of the amendment, the "as soon as practicable" language serves no central purpose in the Title III scheme of safeguards, and a delayed amendment should not result in suppression.[184]

---

[178] *Id.* at 659, 309 N.Y.S.2d at 811. For a further discussion of this case, see note 184 *infra*.

[179] 18 U.S.C. § 2517(5) (1970).

[180] *See* notes 171-74 and accompanying text *supra*.

[181] LEGISLATIVE HISTORY 2189.

[182] *See* notes 173-74 *supra*.

[183] Nothing in the constitutional logic of plain view requires the officer to submit his actions for review, after the search, to a judicial authority. Thus, when surveillance terminates immediately and the only point of an amendment is to allow the judge to determine that the evidence of the new crime was intercepted in the course of an otherwise lawfully conducted wiretap, the amendment procedure is only a statutory requirement and is not mandated by the fourth amendment.

[184] The suppression sanction is built into Title III by 18 U.S.C. §§ 2515, 2518(10)(a) (1970). Section 2515 provides that no part of any intercepted communication or evidence

2. *Surveillance Continues*

When the tap does not end, the amendment may be important to sanction interception of further evidence of the new crime. The matter is not perfectly clear, however, because not every conversation providing evidence of a new crime in the middle of a long wiretap will require the officer in charge to seek an immediate amendment.[185] First, a conversation is not a discrete entity which provides evidence directly attributable to one crime or another.

---

derived therefrom may be admitted in evidence in "any trial, hearing, or other proceeding" if disclosure of the information in question "would be in violation of this chapter." *Id.* § 2515. Section 2518(10)(a) defines what would be in violation of this chapter and grants the defendant the right to suppression on three grounds:

> (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

Id. § 2518(10)(a).

The United States Supreme Court discussed the suppression remedy in the companion cases, United States v. Giordano, 416 U.S. 505 (1974), and United States v. Chavez, 416 U.S. 562 (1974). Read together, the two opinions restrict application of the suppression remedy to violations of sections that "directly and substantially implement" the congressional intent to limit and safeguard the use of wiretaps. 416 U.S. at 527; 416 U.S. at 574-75. For a more detailed discussion of *Giordano* and *Chavez,* see notes 265-73 and accompanying text *infra.*

In the surveillance-terminates case, the timeliness of an amendment is not important and cannot be a direct or substantial safeguard in the Title III scheme to regulate the use of wiretaps. *See* note 183 *supra.* Under the Supreme Court's analysis, then, failure to obtain a timely amendment in the surveillance-terminates case should not result in suppression. People v. Ruffino, 62 Misc. 2d 653, 309 N.Y.S.2d 805 (Sup. Ct. 1970), illustrates this principle. The order authorized interception, for a period of 20 days, of communications relating to narcotics. When the first order expired, the government obtained an extension, again specifying narcotics, and four days later the agents overheard talk of a murder set for that same day. Agents arrested the defendants during the murder attempt and the tap was discontinued. The grand jury returned indictments 12 days later, but the government did not obtain an amendment to cover the interception of the murder conversation until three months after the indictments. *Id.* at 655, 309 N.Y.S.2d at 808. The defendants seized on the opportunity and moved to dismiss the indictments on the ground that the government had not obtained an amendment as soon as practicable. The court denied the motion:

> It seems apparent that the purpose the lawmakers had in mind, in requiring an amendment of an outstanding interception order where new criminal matters . . . came to light over the wiretap, was to legalize the *continuance* [of] the wiretap to discover further evidence of the newly disclosed crimes. Here we are dealing with a situation where the amending order . . . dealt solely with *past* conversations, since the wiretap itself was discontinued immediately upon the overhearing of the "murder" conversation. Under such circumstances . . . I hold that the failure to obtain an amending order as promptly as possible was a mere irregularity which did not affect . . . the prosecutor's right to offer the conversation in evidence. To hold otherwise would exalt form above substance.

Id. at 660, 309 N.Y.S.2d at 812 (emphasis in original).

[185] *See, e.g.,* United States v. Tortorello, 480 F.2d 764, 781-83 (2d Cir.), *cert. denied,* 414 U.S. 866 (1973), where the application for amendment was in effect combined with the application for extension when the authorized period of surveillance expired.

The conversation may be ambiguous or may provide evidence of several crimes, one of which is specified in the warrant, so that the communication might not be plainly outside the scope of the order.[186] Second, a coded conversation overheard near the beginning of the period of interception may only be understood long afterward, far too late to seek a timely amendment.[187] Third, the evidence of a new crime may occur only occasionally, sprinkled throughout a torrent of properly intercepted conversations relating to the specified crime. In such cases the officer in charge of the tap may feel that he is not really looking for evidence of the new crime, that it is being intercepted too infrequently to worry about, and that he does not need an immediate amendment.

The cases are further complicated because the government works with the judge through many channels, and may keep him informally up-to-date on what kinds of material are being intercepted.[188] In a series of progress reports to the judge, the government may disclose that new crimes have been overheard, or the district attorney may make a detailed exposition of new crimes intercepted when he writes affidavits to support an application for extension.[189] Each of these more or less formal contacts with the judge is to some degree a request for judicial sanction of continuing interception of evidence of a new crime, yet none really complies with the statutory form of a special application to the

[186] If a crime is specified in the authorization order, a conversation pertaining to that crime is validly intercepted under that order. No application for amendment is necessary even if the conversation provides evidence of other crimes as well. A conversation validly intercepted under one order could thus be used in a later prosecution for an entirely different purpose, and such later use cannot affect the validity of the original interception.

[187] *See, e.g.,* United States v. Ratenni, 480 F.2d 195, 198-99 (2d Cir. 1973), where certain conversations were not understood until after the tap had been terminated. The court held that "[s]ince the taps had been abandoned there was no necessity to seek a prompt amendment of the original order." *Id.* at 199. Accordingly, the government's failure to ask for the amendment until four months later was not significant and did not call for suppression. *See* note 184 *supra.*

[188] One example of rather casual communication between the judge and the officers executing the surveillance is found in United States v. LaGorga, 336 F. Supp. 190, 194 (W.D. Pa. 1971), where the judge asked for reports on the progress of the tap (under authority granted by 18 U.S.C. § 2518(6) (1970)), and the special attorney in the investigation submitted his reports orally rather than in writing. The district court held that oral reports were not a violation of the statute, since the judge could have dispensed with them entirely, but it noted that "it would be better practice in the future to have communications submitted in writing . . . ." 336 F. Supp. at 194.

[189] The district attorney used the applications for extension as a vehicle for informing the judge of the interception of evidence of new crimes in United States v. Tortorello, 480 F.2d 764, 781-83 (2d Cir.), *cert. denied,* 414 U.S. 866 (1973). The Second Circuit approved and ruled that under the facts of the case no amendment at all was necessary. For a more detailed discussion see notes 199-209 and accompanying text *infra.*

judge. If the judge does not object when informed on several occasions that evidence of a new crime is being intercepted, the prosecutor can later say with some justification that he sought judicial sanction, that it was tacitly given, and that under these circumstances failure to file a formal amendment is of no consequence.

The cases that deal with amendments in the context of continuing surveillance have generally not analyzed the entire problem but have restricted their attention to the facts of the case at bar. Although the result has been a scattering of opinions that conflict with each other to some degree,[190] it is nevertheless possible to construct an amendment theory that accounts for most of the cases.

The inconsistencies in the amendment decisions, as with the minimization cases, stem largely from the infinite variety of wiretap fact patterns. The cases lie on a continuum from clearly inadvertent interception of a single new conversation[191] to clearly intentional interception of an unbroken string of new conversations. From the court's point of view, the spectrum can stretch from an obviously valid case of plain view to an obviously invalid case of a subterfuge search.

At the plain view end of the spectrum, there is probably no need to seek an immediate amendment when a single "new conversation" appears. If the tap has been consistently providing evidence described in the warrant, and there is no reason to expect a significant number of similar new conversations, judicial sanction for further interception of such conversations would be pointless.[192] If, however, the tap has not produced the evidence

[190] *See* United States v. Capra, 501 F.2d 267 (2d Cir. 1974), *cert. denied,* 420 U.S. 990 (1975); United States v. Ratenni, 480 F.2d 195, 198-99 (2d Cir. 1973); United States v. Tortorello, 480 F.2d 764, 781-83 (2d Cir.), *cert. denied,* 414 U.S. 866 (1973); United States v. Lamonge, 458 F.2d 197, 199 (6th Cir.), *cert. denied,* 409 U.S. 863 (1972); United States v. Cox, 449 F.2d 679, 681 (10th Cir. 1971), *cert. denied,* 406 U.S. 934 (1972); United States v. Denisio, 360 F. Supp. 715, 720 (D. Md. 1973); United States v. Sklaroff, 323 F. Supp. 296, 316 (S.D. Fla. 1971), *aff'd,* 506 F.2d 837 (5th Cir. 1975); People v. Di Stephano, 45 App. Div. 2d 56, 356 N.Y.S.2d 316 (1st Dep't 1974); People v. Ruffino, 62 Misc. 2d 653, 309 N.Y.S.2d 805 (Sup. Ct. 1970); People v. Rizzo, 70 Misc. 2d 165, 333 N.Y.S.2d 152 (County Ct. 1972); People v. Sher, 68 Misc. 2d 917, 329 N.Y.S.2d (County Ct. 1972); People v. Di Lorenzo, 69 Misc. 2d 645, 330 N.Y.S.2d 720 (County Ct. 1971).

[191] As used in this Comment, a new conversation is one which provides evidence of a new crime.

[192] An example of a case where an immediate amendment should not have been necessary is United States v. Ratenni, 480 F.2d 195, 198-99 (2d Cir. 1973). In this case the tap continued in operation for two and one-half months, but the conversations which the defendants insisted were new and required an immediate amendment occurred on four days

expected, or if the officer in charge has probable cause to believe that the new conversation is likely to recur frequently, then an immediate amendment is probably required.[193]

At the subterfuge end of the spectrum is the situation where great volumes of incriminating material not described in the warrant appear.[194] Particularly if little or no expected evidence appears, or if law enforcement officers begin to track down the leads provided in the new conversations, an amendment or even an entirely new warrant should be required.[195]

A court, in passing on the question of whether the government obtained a timely amendment, should consider a number of

---

within the space of a week. In the actual case the monitoring agents did not understand the conversations until later, so they could not have applied for an amendment at the time. *See* note 187 *supra*. Even if the officers had immediately understood the conversations, the calls occurred so infrequently and within such a short space of time that they seem to have been picked up purely incidentally. The government was not interested in the conversations until later; the agents on the spot apparently did not expect substantial further interception of similar communications; and the tap had produced useful evidence of the type described in the warrant. Under these circumstances, the government should not have had to amend the warrant immediately and could validly have done so at any time after the termination of surveillance. Nevertheless, the safest course for the government is to obtain the amendment immediately.

[193] If the tap has not produced the evidence expected, then it is susceptible to attack on the ground that it was a subterfuge search for any evidence of any crime which might turn up. The government in such cases must protect itself by swiftly moving to amend the order to reflect the crimes which actually appear. If the officer in charge suspects that the new conversation is likely to recur frequently, then he must request a prospective amendment and support the application with a showing of probable cause. *See* note 174 *supra;* People v. Di Stephano, 45 App. Div. 2d 56, 60, 356 N.Y.S.2d 316, 320 (1st Dep't 1974). This case has been appealed to the New York Court of Appeals and is expected to be decided shortly.

[194] Although an immediate amendment was not filed in United States v. Denisio, 360 F. Supp. 715, 719 (D. Md. 1973), and the court declined to suppress, *Denisio* is a paradigm of the situation in which immediate amendment should be required. The authorization order specified robbery, bribery, and conspiracy, but the agents intercepted nothing but evidence of bookmaking activities. Six months later federal authorities obtained an amendment for the first time on the eve of trial. The district court adopted a unique view of the amendment procedure, ruling that the timeliness of the application bore only on the judge's initial decision to approve it and did not affect its validity on subsequent review. *Id.* at 720. This approach apparently would preclude an appellate review of the timeliness issue and has not been adopted by other courts which have considered themselves free to inquire into the timeliness of an amendment.

[195] In People v. Rizzo, 70 Misc. 2d 165, 333 N.Y.S.2d 152 (County Ct. 1972), the district attorney obtained an entirely new authorization order when a new name appeared in conversations intercepted under the old order. The defendants argued that the old order had never been properly amended, but the court ruled that a new order

> is stronger than an amended warrant. The District Attorney could have chosen to amend the original warrant to include the evidence derived against this defendant as a result of the intercepted communications not part of the original warrant. He chose, however, to obtain a new warrant which, in this Court's opinion, served the same purpose as an amendment and was, in fact, a stronger document.

Id. at 166, 333 N.Y.S.2d at 153.

factors. First, the court should evaluate how difficult it was to distinguish the new conversations from the expected conversations, how closely the two offenses were linked, how difficult it was for the agents on the spot to understand the subject matter of discussion, and whether the new conversations were arguably pertinent to the originally authorized investigation. This inquiry would lead the court to determine whether the monitoring officers should have realized immediately that they were intercepting material not covered in the warrant. If there was good cause for confusion in the minds of the agents, then a delay in seeking an amendment is more easily understood and permitted. However, if there is reason to believe the agents knew they were intercepting new conversations, but deliberately chose not to seek an amendment, then delay is less easily tolerated.

Second, the court should consider the degree to which the tap's output conformed to the description in the warrant. When the tap produces the expected information, then the original warrant appears to be legitimate even if a new crime is uncovered. But if a narcotics wiretap yields no evidence at all prior to perception of gambling evidence, or yields nothing but evidence of gambling, the investigation is actually a gambling investigation under a narcotics warrant.[196] In the most extreme cases, it would be safest for the government to obtain an entirely new warrant, despite the overwhelming paperwork involved.[197]

[196] *See* United States v. Denisio, 360 F. Supp. 715, 719 (D. Md. 1973). This case is discussed in note 194 *supra*. In People v. Di Lorenzo, 69 Misc. 2d 645, 330 N.Y.S.2d 720 (County Ct. 1971), the court explained its holding that a failure to obtain an immediate amendment must result in suppression in the following terms:

> The invasion of an individual's right of privacy is not to be lightly condoned, whether it involves the person himself, his dwelling or his telephone conversations. It is permissible only when there is probable cause that a crime is being committed. Thus, when the interception of a conversation discloses that a crime not contained in the eavesdropping warrant is being committed, an order amending the eavesdropping warrant should be immediately obtained and surveillance continued only after a judicial determination of probable cause that the new crime is being committed.

Id. at 651, 330 N.Y.S.2d at 727. The statement is overly broad in that it appears to contemplate a bar on interception of all new conversations until an amendment is obtained. The discussion thus far indicates that there are many situations in which surveillance could be continued without an immediate amendment, however, and no other court so far has adopted this court's strict reading of the statutory language. Nonetheless this court is one of the few to recognize that an immediate amendment based on a showing of probable cause may in certain situations be a constitutional necessity to legitimize continued interception of new conversations.

[197] *See* note 195 *supra*. When the government amends the order to permit future interception of new conversations, it is in effect a new order and must show probable cause. In the most extreme cases, however, the government should protect its case by beginning the application process anew and requesting an entirely new order.

Third, the court should consider whether the agents made efforts to inform the judge that new conversations were being intercepted. Even if a formal amendment was not filed until after the end of the tap, the purpose of obtaining judicial approval of continuing surveillance can be achieved through informal conversations with the judge, periodic progress reports, or an application for an extension.[198]

Fourth, the court should consider the extent of the delay. If the amendment was obtained two weeks after the first new conversation but one month before the end of surveillance, little harm has been done and the government has obtained advance judicial approval for a sizeable period of surveillance. If the amendment is delayed until after the termination of surveillance, however, the constitutional demand for advance judicial approval of a search may have been thwarted, and the argument for suppression is stronger.

Although no court so far has expressly employed these four factors in its evaluation of an amendment case, many of the cases would have been decided the same way if the court had done so.[199] One of the leading decisions is the Second Circuit's opinion in *United States v. Tortorello.*[200] Interception began under a New York authorization order that listed a variety of crimes, including grand larceny.[201] Surveillance continued for 149 days under five extensions of the order.[202] The tap apparently produced useful

[198] *See* notes 188, 189 and accompanying text *supra*. Even if the officer in charge of the wiretap has not filed an application for an amendment, he must make the equivalent of such an application if he applies for an extension of the period of surveillance. According to 18 U.S.C. § 2518(5) (1970), applications for extension stand on the same footing as applications for the original order. Thus, all the provisions requiring showings of probable cause and particular description of the crime apply to applications for extension. If the monitoring agents intercept new conversations during the first period of surveillance, then it is usually clear that interceptions of similar conversations may occur in the future. The strict language of § 2518(4), requiring that orders specify the crime with particularity, would then require the applicant to detail what evidence had been intercepted in the first period of surveillance.

Moreover, § 2518(1)(f) provides: "Each application shall include the following information: . . . (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception . . . ." Thus, an application for extension must include a request to add any new crimes to those specified in the first order, so that the new order meets the § 2518(4)(c) particularity requirement. This duty is wholly independent of the § 2517(5) amendment requirement, but the extension may in certain cases take the place of the amendment. *See* note 189 *supra* and notes 200-09 and accompanying text *infra*.

[199] One case which would have been decided differently is United States v. Denisio, 360 F. Supp. 715, 719-20 (D. Md. 1973), discussed in note 194 *supra*.

[200] 480 F.2d 764 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973).

[201] *Id.* at 770-71.

[202] *Id.* at 771.

evidence of the types described in the original order, but after the first extension, the agents also began periodically overhearing evidence that Tortorello was planning violations of federal securities laws.[203] Representatives of the Securities and Exchange Commission and the Justice Department joined the surveillance team, and interception of the stock fraud conversations continued throughout the remainder of the tap.[204] The district attorney never filed an application for an amendment, but he fully informed the judge of the continuing interception of stock fraud conversations in each application for an extension.[205] On appeal, the court agreed that the government had supplied enough information to enable the judge to rule on the tap's lawfulness, and therefore declined to suppress despite a complete failure to apply for an amendment.[206] The defendant further objected that the wording of the six successive authorization orders was never changed to include securities violations in the list of designated offenses. The government responded that a wording change was unnecessary because the order was issued under New York law, the securities violations were federal offenses, and grand larceny was the closest any state offense could come to covering the stock fraud scheme.[207] The government further pointed out that the extension orders incorporated by reference the district attorney's affidavits, which contained a complete statement of the stock fraud conversations. The court accepted the government's position on this point as well.[208]

Since the judge in this case was given four formal opportunities to pass on the propriety of continued interception of the stock fraud conversations, it would appear that the underlying purposes of the statute were fully satisfied and the court reached the proper result. For instance, there were no signs that the original authorization was a subterfuge. It appears from the opinion that the tap produced considerable evidence of the type described in the authorization order, and so did not become primarily an investigation into Tortorello's stock scheme. It would thus seem that the officer in charge of the tap was justified in failing to obtain an amendment. Nonetheless, it would have been better practice, from both the defendant's and the government's

[203] *Id.* at 782.
[204] *Id.* at 771.
[205] *Id.* at 781-82.
[206] *Id.* at 782-83.
[207] *Id.*
[208] *Id.*

standpoints, for the district attorney to have obtained an immediate, formal amendment as soon as he realized that the tap was likely to continue to collect stock fraud evidence.[209]

In contrast to *Tortorello,* at least one court has construed the language of the statute strictly. In *People v. Di Lorenzo,*[210] the court ruled that an amendment must be sought "immediately" or interception of the new crime must cease.[211] The court's reasoning is defective, however, for failure to take account of the plain view exception to the strict requirements of probable cause.[212] To date, no other court has adopted such an inflexible reading of the statute.[213]

B. *New Person*

The fourth amendment requires that the warrant describe with particularity the place to be searched and the things to be seized. It does not, however, require the warrant to name the owner or occupant of the place to be searched. In the wiretap analogy, the place to be searched is the telephone number, and the

[209] Although the applications for extension in *Tortorello* contained all the information that would have been contained in an application for an amendment, the application for an extension neither focuses the judge's attention on an evaluation of the lawfulness of prior interception of new conversations, nor asks specifically that the judge approve future interception of similar new conversations. Although the judge in *Tortorello* made no objection to the interception of the stock fraud conversations, he may not have been aware that he was tacitly approving those interceptions; indeed, he never altered the wording of the order to include stock fraud, nor did he ever take any action that could be seen as positive approval rather than passive acceptance. An application for an amendment, on the other hand, would focus the judge's attention on the specific question of whether past interceptions of new conversations were lawful, and whether he would approve of future interception of such conversations. The ambiguity of "tacit approval" would be eliminated, and it would be clear that the judge had considered the interceptions and approved them.

It is now clear that the standard to be used in evaluating the execution of a wiretap is the contemporaneous perspective of the reasonable agent on the spot. Both in the minimization and amendment contexts, the court will not impose its hindsight on the officers who had to make occasionally difficult decisions without time to ponder them. *See* United States v. Scott, 504 F.2d 194, 198 (D.C. Cir. 1974) (promulgating the contemporaneous standard in a minimization case). From this point of view, an application for an amendment while the tap is in progress gives the judge a chance to evaluate the agents' performance from their contemporaneous perspective. Approval of the application can thus be an important line of defense for the prosecution if the defendants charge that the tap was not lawfully executed.

[210] 69 Misc. 2d 645, 330 N.Y.S.2d 720 (County Ct. 1971).

[211] *Id.* at 652, 330 N.Y.S.2d at 727.

[212] When the new crime is intercepted as evidence in "plain view" during the course of a lawful wiretap, interception need not cease until an amendment is obtained. *See* notes 191-98 and accompanying text *supra.*

[213] *But see* United States v. Capra, 501 F.2d 267, 276-77 (2d Cir. 1974), *cert. denied,* 420 U.S. 990 (1975) (New York law requires immediate amendment of warrant to add new person).

things to be seized are conversations of a particular type. Thus there appears to be no constitutional requirement that the warrant set out with particularity the names of the persons whose conversations are sought.[214]

Title III requires that the order contain "a particular description of the type of communication sought,"[215] but only requires specification of "the identity of the person, if known, whose communications are to be intercepted."[216] Although defendants have frequently challenged this dichotomy in the level of particularity required, the distinction has withstood attack, and the courts have regularly held that interception and use of conversations of persons not named in the order is both constitutionally and statutorily permissible.[217]

Occasionally, defendants have further maintained that the amendment requirement applies to the discovery of a new person as well as a new crime. The courts have rejected this contention, however, and have properly ruled that an amendment is only required in the case of a new crime.[218] Title III provides that an amendment is required when a law enforcement officer intercepts "wire or oral communications relating to *offenses* other than those specified in the order of authorization," but makes no mention of persons not named in the order.[219]

---

[214] Although the Federal Constitution would not require particularization of the names of the suspects, New York has added a wiretap analogue to its state constitution which does make such a requirement. N.Y. CONST. art. I, § 12. However, the New York Court of Appeals has construed this section to permit interception of communications of persons not named in the warrant. People v. Gnozzo, 31 N.Y.2d 134, 144-45, 286 N.E.2d 706, 711, 335 N.Y.S.2d 257, 264 (1972), *cert. denied,* 410 U.S. 943 (1973). *But see* United States v. Capra, 501 F.2d 267, 276-77 (2d Cir. 1974), *cert. denied,* 420 U.S. 990 (1975).

[215] 18 U.S.C. § 2518(4)(c) (1970).

[216] *Id.* § 2518(4)(a).

[217] *See* United States v. Cox, 449 F.2d 679, 686-87 (10th Cir. 1971), *cert. denied,* 406 U.S. 934 (1972); United States v. Iannelli, 339 F. Supp. 171, 177 (W.D. Pa. 1972), *aff'd on other grounds,* 477 F.2d 999 (3d Cir. 1973), *aff'd,* 420 U.S. 770 (1975); United States v. LaGorga, 336 F. Supp. 190, 192-93 (W.D. Pa. 1971); People v. Gnozzo, 31 N.Y.2d 134, 286 N.E.2d 706, 335 N.Y.S.2d 257 (1972), *cert. denied,* 410 U.S. 943 (1973).

[218] *See, e.g.*, United States v. O'Neill, 497 F.2d 1020, 1023-24 (6th Cir. 1974); People v. Gnozzo, 31 N.Y.2d 134, 286 N.E.2d 706, 335 N.Y.S.2d 257 (1972), *cert. denied,* 410 U.S. 943 (1973); People v. Ruffino, 62 Misc. 2d 653, 659, 309 N.Y.S.2d 805, 811 (Sup. Ct. 1970). *But see* United States v. Capra, 501 F.2d 267, 276-77 (2d Cir. 1974), *cert. denied,* 420 U.S. 990 (1975).

[219] 18 U.S.C. § 2517(5) (1970) (emphasis added). The New York statute, which is nearly identical to Title III, requires an amendment when a law enforcement officer intercepts a "communication which was not otherwise sought." N.Y. CRIM. PRO. LAW § 700.65(4) (McKinney 1971). The New York Court of Appeals has construed this language to mean only conversations yielding evidence of a new crime:

> Where the communication intercepted involves the crime specified in the warrant,

Since it is often the very purpose of a wiretap to explore the extent and identity of a conspiracy, the authorization order may specify conversations of several named suspects, "and others as yet unknown."[220] In such cases it is clear that conversations of persons not named in the warrant are precisely the things sought, and it would serve no purpose to require the agents to obtain an amendment each time they ascertain a new name.[221] It is clear that amendments for new names are not required, and that if a conversation is otherwise validly intercepted, it is not made invalid because both parties are not named in the authorization order.

III

SEALING

One of the less frequently litigated sections of Title III requires the government to present the tapes to the issuing judge "immediately upon the expiration of the period of the order," so that they may be "sealed under his directions."[222] The presence of the seal, "or a satisfactory explanation for the absence thereof," is a prerequisite to the use of the tapes in evidence.[223] Applications and

---

> the named suspect, and an unknown outside party, . . . the communication is "sought" and no amendment is required . . . .
>
> . . . Thus, the legislative intent was to require amendments where different crimes are disclosed.

People v. Gnozzo, 31 N.Y.2d 134, 143-44, 286 N.E.2d 706, 710, 335 N.Y.S.2d 257, 263 (1972), *cert. denied*, 410 U.S 943 (1973).

[220] *See* United States v. Kahn, 415 U.S. 143, 146 (1974). Although the question in the case was the construction of the phrase, "and others as yet unknown," and not its validity, the Court implied that such a grant of authority was proper. *Id.* at 153-55. *See* United States v. Fiorella, 468 F.2d 688, 691 (2d Cir. 1972), *cert. denied*, 417 U.S. 917 (1974) (approving use of "others as yet unknown" in the authorization order).

[221] Although an amendment is unnecessary each time a new name appears, the government is under an obligation to add to the order the names it knows when it applies for an extension. Since the extension is governed by the same rules as the original order, the government must specify "the identity of the person, if known, whose communications are to be intercepted." 18 U.S.C. § 2518(4)(a) (1970). If the government is aware of new names of suspects when it applies for an extension, then this statutory language would require that those names be set out in the order. Furthermore, if the original language of the order specifies one or more names "and others as yet unknown," and that language was not changed when the tap was extended, then new names discovered during the first period of surveillance would not be subject to interception. The new names would be neither the names originally specified, nor "others as yet unknown," and neither category in the order would cover the new names which were not added at extension time. *Cf.* United States v. Kahn, 415 U.S. 143, 149-58 (1974); United States v. O'Neill, 497 F.2d 1020, 1023-25 (6th Cir. 1974).

[222] 18 U.S.C. § 2518(8)(a) (1970).

[223] *Id.*

orders must also be "sealed by the Judge."[224] The purposes of the sealing requirement are to prevent the tapes and documents from being altered or tampered with, to ensure that the contents remain confidential, and to help establish the chain of custody.[225]

Although minor variances from the exact requirements of the statute will not result in suppression,[226] a more serious infraction may incur the court's wrath. In *People v. Nicoletti*[227] the monitoring agents failed to present the tapes to the issuing judge for sealing. A police detective kept the tapes in a locked footlocker in his home, made duplicate recordings of certain portions, and with the district attorney and other police officers, made transcripts of the conversations.[228] Although the New York authorities argued that there was substantial compliance with the statute; that the issuing judge was told of the storage arrangements; that the tapes were needed for transcription; and that no secure storage facility was available, the New York Court of Appeals ruled that the violation was serious and that the evidence would be suppressed.[229]

---

[224] *Id.* United States v. Cantor, 470 F.2d 890 (3d Cir. 1972), addressed the question of the exact meaning of "sealed by the judge." Instead of sealing the application and order himself, the judge gave the documents to an agent and told him to place them in an envelope, seal them, and store them. The agent did so, but did not seal the envelope until after he had left the judge's chambers. The defendant argued that this procedure was not what the statute called for, and that only the judge could perform the actual sealing process. *Id.* at 892-93. The Third Circuit disagreed. Noting that there was no claim that the documents had been altered, and that the procedure actually followed conformed to the statute in all except minor details, the court concluded: "While it would have been more appropriate, and we recommend it for the future, for the judge rather than the agent to have sealed the documents, his sealing would not have added to the confidentiality of the documents."

[225] *Id.* at 893. United States v. Kohne, 358 F. Supp. 1053, 1058 (W.D. Pa.), *aff'd*, 485 F.2d 682 (3d Cir. 1973), *cert. denied*, 416 U.S. 957 (1974); People v. Nicoletti, 34 N.Y.2d 249, 253, 313 N.E.2d 336, 338, 356 N.Y.S.2d 855, 858 (1974).

[226] *See* United States v. Poeta, 455 F.2d 117, 122 (2d Cir.), *cert. denied*, 406 U.S. 948 (1972). When the wiretap in this case was completed, the judge who issued the order was on vacation, and the applicable New York statute directs that the tapes be sealed under the direction of the "issuing justice." N.Y. CRIM. PRO. LAW § 700.50(2) (McKinney 1971). The police waited 13 days and then presented the tapes to another judge to be sealed. The Second Circuit concluded:

> Section 2518(8)(a) [of Title III] provides that in the absence of a seal the tapes might be used in evidence if 'a satisfactory explanation for the absence' is made. *A fortiori*, where, as here, the tapes are sealed, a satisfactory explanation for the delay will allow their use in evidence. We are satisfied that the delay of the police in delivering the tapes for sealing was entirely excusable . . . .

455 F.2d at 122. *Accord*, Commonwealth v. Vitello, 327 N.E.2d 819, 849-50 (Mass. 1975). *See also* United States v. Sklaroff, 506 F.2d 837, 840 (5th Cir. 1975) (delay of 14 days permitted); People v. Blanda, 80 Misc. 2d 79, 362 N.Y.S.2d 735 (Sup. Ct. 1974) (two day delay permitted); Cranwell, *supra* note 11, at 254-55.

[227] 34 N.Y.2d 249, 313 N.E.2d 336, 356 N.Y.S.2d 855 (1974).

[228] *Id.* at 252, 313 N.E.2d at 337-38, 356 N.Y.S.2d at 857.

[229] *Id.* at 252-53, 313 N.E.2d at 338, 356 N.Y.S.2d at 857-58.

> Measured against the potential for abuse, the explanations offered in this case are patently insufficient. While the parties charged with custody of the tape recordings were cognizant of the sealing requirement, they did not present them to the issuing Justice . . . as was their duty. That the issuing Justice was advised of the custody arrangements will not suffice. While he may have tacitly approved them, the fact remains that the recordings were not sealed. . . . [D]uplicate recordings could and should have been made and the originals preserved under seal.[230]

Because the police had played and replayed the unsealed originals, there was a "possibility for human or mechanical error."[231] The court therefore decided that the statute had been seriously violated and that the tapes were improperly admitted into evidence.[232]

IV

INVENTORIES

After surveillance is over and the tapes are sealed, the issuing judge must order service of an inventory notice on the persons named in the eavesdropping order. The inventory must include the fact that the eavesdropping order was issued, the date it was issued, the period for which interception was authorized, and a statement of whether or not the individual's conversations were intercepted. The inventory must be served within ninety days after termination of the tap. The issuing judge is given discretion to determine whether to require service of inventories on persons not named in the eavesdropping order, and any judge of competent jurisdiction may, upon an *ex parte* showing of good cause, postpone service of any inventory.[233]

The statutory scheme and its demands on law enforcement officers seem simple and easily complied with. All the officer in charge of the investigation need do is serve a straightforward document on a specified group of people plus any other persons the judge may require.[234] If the officer feels that service should be

---

[230] *Id.* at 253, 313 N.E.2d at 338-39, 356 N.Y.S.2d at 858 (footnotes omitted).

[231] *Id.* at 254, 313 N.E.2d at 339, 356 N.Y.S.2d at 858.

[232] *But see* United States v. Falcone, 505 F.2d 478, 483-84 (3d Cir. 1974) (improper sealing procedures may not result in suppression since the sealing process cannot affect the lawfulness of the original interception).

[233] The inventory notice requirements are set forth in 18 U.S.C. § 2518(8)(d) (1970).

[234] The statute places the duty upon the judge to cause service of the inventory, but as a practical matter the burden falls upon the prosecutor. If the inventory is not served within the 90-day limit, there is a chance that the wiretap evidence will be suppressed. The prosecutor thus risks losing his case if he fails to ensure that the judge orders federal marshals to make service within the statutory deadline.

delayed for any good reason, he need only request any competent judge to postpone the deadline, and judges in practice never refuse.[235] In theory, law enforcement officers should routinely comply with this section and inventories should never be the subject of litigation. In fact, the wiretap cases reveal a sorry record of frequent noncompliance.[236] Officers have often served inventories beyond the statutory ninety day limit or not at all, and defendants have been quick to seize on the government's failure as a ground for suppression. The issues presented by the motion to suppress in the inventory cases are more subtle than they might appear. Many of the courts considering this problem have disposed of it with only cursory analysis and have not considered the possibilities that post-termination notice may be a constitutional requirement,[237] that notice may be constitutionally required to persons not named in the authorization order despite the judge's apparent discretion, and that different varieties of failure to provide notice present different issues.[238]

Although the literal language of the fourth amendment makes no requirement of either pre- or post-search notice, the common law and the Federal Rules of Criminal Procedure both make some kind of notice requirement.[239] The reason, evidently, is that secret searches are alien to the democratic tradition and notice to persons facing criminal prosecution is a fundamental element of due process.[240] Thus the cases that consider the constitutional

---

[235] 18 U.S.C. § 2518(8)(d) (1970).

[236] It is easy to speculate on why violations occur. Officers manning a wiretap investigation are usually overworked and may simply forget to serve inventories. For a description of how much work is entailed in the day-to-day execution of a wiretap, see United States v. Falcone, 364 F. Supp. 877, 880-81 (D.N.J. 1973). Sometimes the defendants learn of the wiretap through their own sources of information, move for discovery or suppression and thus reveal their awareness of the tap, and the investigating officers may assume service of the inventory is unnecessary. *See, e.g.*, United States v. Wolk, 466 F.2d 1143, 1144 (8th Cir. 1972).

[237] Significant consequences result from a decision that the inventory notice provision is of constitutional dimension. *See* notes 243-46 and accompanying text *infra*.

[238] In United States v. Lawson, 334 F. Supp. 612 (E.D. Pa. 1971), for instance, the court dismissed the defendant's contention that the inventory had been filed late:

> Existing practice with regard to returning and filing search warrants is persuasive authority for determination of procedures under § 2518. The return and filing of a search warrant are ministerial acts, . . . and absent a substantiated claim of prejudice, failure to file a warrant should not invalidate an otherwise lawful search.

Id. at 616.

[239] *See* A.B.A. MINIMUM STANDARDS 91-92. *Cf.* Ker v. California, 374 U.S. 23, 38-39 (1963); Miller v. United States, 357 U.S. 301, 305-06 (1958) (discussing requirements that officers announce identity and purpose before entry to make search); FED. R. CRIM. PRO. 41(d) (requiring officer to give copy of warrant to person whose premises were searched).

[240] The senate report accompanying Title III states:

implications of notice in the wiretap situation indicate that post-termination notice is a factor bearing on the reasonableness, and therefore constitutionality, of the wiretap.[241]

Although the Supreme Court in *Berger* did not hold plainly that notice is a constitutional requirement, it listed a number of apparently constitutional objections to the permissive New York statute. Concluding the list, the Court stated:

> Finally, the statute's procedure, necessarily because its success depends on secrecy, has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts. . . . Nor does the statute provide for a return on the warrant thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties. In short, the statute's blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures.[242]

A recent opinion from the Ninth Circuit treated this language as establishing a constitutional notice requirement,[243] and the legislative history of Title III reveals that the congressional draftsmen interpreted *Berger* in the same way.[244]

Although the constitutional requirement would certainly be fulfilled by prompt post-termination notice to all persons whose communications had been intercepted, no one has argued that the Constitution sweeps this broadly. Title III fashions the requirement along more restricted lines.[245] Since there is no reason to suppose

---

> [T]he intent of the [notice] provision is that the principle of post-use notice will be retained. This provision alone should insure the community that the techniques are reasonably employed. Through its operation all authorized interceptions must eventually become known at least to the subject.

LEGISLATIVE HISTORY 2194.

Commenting on their prototype of the Title III notice requirement, the A.B.A. Minimum Standards group wrote: "The principle . . . should itself always remain that post-use notice would have to be given at some time. The possibility of surreptitious surveillance is, of course, the most telling objection to any system of permissive use." A.B.A. MINIMUM STANDARDS 161.

[241] It would appear that in the literal context of the Fourth Amendment, post-search notice of an electronic interception may properly relate only to the issue of 'reasonableness' in the conduct of 'searches and seizures.'. . .

> . . . [T]he constitutional standard for searches and seizures relating to both tangible objects and communications is the reasonableness of the governmental action. Only unreasonable searches and seizures are beyond the constitutional pale.

United States v. Cafero, 473 F.2d 489, 500 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974). *See* United States v. Whitaker, 474 F.2d 1246, 1247 (3d Cir.), *cert. denied*, 412 U.S. 953 (1973).

[242] Berger v. New York, 388 U.S. 41, 60 (1967).

[243] United States v. Chun, 503 F.2d 533, 536-37 (9th Cir. 1974).

[244] LEGISLATIVE HISTORY 2161-62.

[245] Notice must be served within 90 days on persons named in the authorization order.

that the Constitution requires more than actual notice, it is possible to violate the statute without violating the Constitution. If the inventory is not in the prescribed form, or if it is not served within the ninety day limit, the government has violated the statute, but actual notice, whether from an inventory or from some other source, should nonetheless comply with the Constitution.[246]

When the government fails to serve the inventory on time, the courts have been faced with the dilemma of either permitting a clear violation of the statute or declaring that a wiretap that was valid when executed became invalid through the operation of a condition subsequent.[247] The courts have understandably been very reluctant to allow a violation that occurred after the wiretap to cause suppression of all the evidence previously acquired by valid means; the violation seems minor, the cost of gathering the evidence might have been great, and the government might not have a case if it could not use the wiretap tapes in evidence. Nevertheless, several courts have decided that some violations were too blatant or too important to permit and have ordered suppression.[248]

The cases can best be discussed in five different categories according to their facts.

A. *Lengthy Postponements*

In some cases defendants have requested suppression on the ground that the judge repeatedly postponed the deadline for serving the inventory. In one case notice was postponed until six months after the termination of surveillance, and the defendants argued that the judge had abused his discretion by permitting notice to be so delayed.[249] In this and in similar cases, however, the

---

The judge may exercise his discretion to postpone the deadline for service, however, and may order service of notice on other persons. 18 U.S.C. § 2518(d) (1970).

[246] One court has stated that the fourth amendment requires notice

> including at a minimum all the information contained in a subparagraph 2518(8)(d) inventory notice given promptly after the decision to obtain an indictment has been made. What constitutes "promptly" should focus on whether the individual has been afforded a reasonable opportunity to prepare an adequate response to the evidence derived from the interception.

United States v. Chun, 386 F. Supp. 91, 93 (D. Hawaii 1974).

[247] *See* United States v. Cafero, 473 F.2d 489, 499 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

[248] Out of the 13 cases from New York and the federal courts dealing with some facet of notice, only three have ordered suppression: United States v. Donovan, 513 F.2d 337 (6th Cir. 1975); United States v. Eastman, 465 F.2d 1057 (3d Cir. 1972); United States v. Chun, 386 F. Supp. 91 (D. Hawaii 1974).

[249] United States v. Manfredi, 488 F.2d 588, 601 (2d Cir. 1973), *cert. denied*, 417 U.S. 936 (1974).

appellate courts have refused to find an abuse of discretion and have agreed that the delay was justified.[250] The reason for lengthy delays most frequently cited is that an ongoing investigation necessitates continued secrecy.[251] Successive overlapping wiretaps of related persons also constitutes good cause for delaying service.[252] If the first suspect were notified that his telephone had been tapped, he would quickly transmit that fact to the others, and the ongoing wiretaps would be useless.

Excessive postponement for no good cause, however, might well warrant a court to find an abuse of discretion and order suppression. The Third Circuit in *United States v. Cafero*[253] warned that judges "should exercise great care" in granting extensions beyond the ninety-day period.[254] Law enforcement officers seeking to secure convictions should not request postponements unless they can show a legitimate reason for delay. Postponements are not a violation of the statute per se since the judge is granted discretion in this regard, but defendants can always challenge the exercise of discretion. The prosecution has won so far, but administrative convenience or overworked staff are arguments unlikely to persuade a skeptical appellate court that an inventory could not have been served within ninety days.

B. *Late Service*

In this category of cases the inventory is not served within the ninety-day limit or within the eventual limit established by judicial postponement, but it is actually served. Late service is a clear violation of the statute, but is probably not a constitutional violation because actual notice is provided.[255] Decisions in this category have appeared regularly throughout the history of Title III, and courts have just as regularly declined to suppress.[256] On the whole,

---

[250] *See, e.g.*, United States v. Cafero, 473 F.2d 489, 500 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974); United States v. Curreri, 363 F. Supp. 430, 436 (D. Md. 1973); United States v. Lawson, 334 F. Supp. 612, 616 (E.D. Pa. 1971).

[251] *See, e.g.*, United States v. Lawson, 334 F. Supp. 612, 616 (E.D. Pa. 1971).

[252] *See, e.g.*, United States v. Curreri, 363 F. Supp. 430, 436 (D. Md. 1973).

[253] 473 F.2d 489 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

[254] *Id.* at 500.

[255] Although the fourth amendment has been read to require notice, the notice need be in no particular form and must simply be sufficient to afford the individual a reasonable opportunity to prepare an adequate response to the evidence derived from the wiretap. *See* United States v. Chun, 503 F.2d 533, 538 (9th Cir. 1974).

[256] *See, e.g.*, United States v. Wolk, 466 F.2d 1143, 1144-46 (8th Cir. 1972); United States v. Schullo, 363 F. Supp. 246 (D. Minn. 1973), *aff'd on other grounds*, 508 F.2d 1200 (8th Cir. 1975), *cert. denied*, 421 U.S. 947 (1975); United States v. Lawson, 334 F. Supp. 612, 616-17 (E.D. Pa. 1971).

however, the rationale used to support their refusal to suppress has been very weak.

Earlier cases made an analogy between the wiretap inventory and a search warrant return, reasoning that the analogy was proper because both documents were filed after the search had been made.[257] Since the search warrant return is universally held to be a mere ministerial duty,[258] several courts reasoned that the inventory is also a ministerial duty, and suppression would not follow unless the defendant could show prejudice resulting from the delay.[259] The analogy is defective, however. Whereas a search for tangible evidence is normally preceded by notice, leaving the post-search return of secondary importance, the wiretap inventory is the first and only notice given. The tap must be secret while it is in progress, so the lack of pre-wiretap notice places far greater significance on the post-wiretap notice procedure.[260] Because the search warrant return does not inform the persons involved for the first time, it has not been thought to be constitutionally required,[261] but the Supreme Court has held that post-termination wiretap notice is of constitutional dimension.[262] The inventory provisions of Title III, therefore, cannot be dismissed as ministerial duties, because those provisions were included in the statute to satisfy a constitutional requirement.[263]

A much better view is to recognize that both constitutional and statutory authority govern the inventory, and that a late inventory is a violation of the statute but probably is not a violation of the Constitution.[264] Not all violations of Title III warrant suppression of evidence, however, as the Supreme Court has recently made clear in *United States v. Giordano*[265] and its companion case, *United States v. Chavez.*[266]

These two cases, although addressing a different section of

---

[257] *See, e.g.*, United States v. Cafero, 473 F.2d 489, 499-500 (3d Cir. 1973).

[258] *See, e.g.*, Evans v. United States, 242 F.2d 534 (6th Cir.), *cert. denied*, 353 U.S. 976 (1957); United States v. Avarell, 296 F. Supp. 1004, 1014 (E.D.N.Y. 1969) (two and one-half year delay in filing a search warrant return and inventory permitted).

[259] The language in United States v. Lawson, 334 F. Supp. 612, 616 (E.D. Pa. 1971), is typical. *See* note 238 *supra*. *See also* Commonwealth v. Vitello, 327 N.E.2d 819, 848-49 (Mass. 1975).

[260] *See* United States v. Chun, 503 F.2d 533, 537 n.6 (9th Cir. 1974).

[261] United States v. Cafero, 473 F.2d 489, 499 (3d Cir. 1973).

[262] Berger v. New York, 388 U.S. 41, 60 (1967). *See* United States v. Chun, 503 F.2d 533, 536-37 (9th Cir. 1974).

[263] *See* notes 242-44 and accompanying text *supra*.

[264] *See* note 255 and accompanying text *supra*.

[265] 416 U.S. 505 (1974).

[266] 416 U.S. 562 (1974).

Title III, provide a blueprint for determining whether a particular violation should lead to suppression. The court ruled that if the section violated does not "directly and substantially"[267] implement Title III's scheme to prevent abuse of wiretaps,[268] then the violation should not result in suppression.[269] If the section is a central safeguard, then violation of that section may warrant suppression, but further inquiry is necessary. The Court's second consideration is whether the section's purpose has been satisfied despite the violation—in other words whether there has been substantial compliance with the statutory purpose.[270] If the matter is still not settled, at least one court reads *Chavez* to suggest that inquiry may progress to whether the government intentionally violated the section, and if so, whether the purpose was to gain a tactical advantage.[271]

In *United States v. Chun*[272] the Ninth Circuit held squarely that the inventory provision of Title III "is a central or at least a functional safeguard in the statutory scheme."[273] The court based its holding on the constitutional necessity of notice and the peculiar necessity of post-search notice in the wiretap situation to avoid secret searches.[274] This conclusion renders suppression possible and necessitates consideration of the second criterion.

It is because of this second inquiry—whether the statutory purpose has been achieved—that the courts have been correct in their refusal to suppress due to late service. Whether or not the inventory was served precisely within the statutory limit is usually of no moment whatsoever to the defendant, and the statutory purpose—actual notice—is satisfied when the inventory is served.

It is possible, of course, that service could be delayed so long that the defendant is prejudiced in his defense.[275] In such a case

---

[267] United States v. Giordano, 416 U.S. 505, 527 (1974).

[268] See the discussion of the *Giordano-Chavez* analysis in United States v. Chun, 503 F.2d 533, 541-42 (9th Cir. 1974).

[269] United States v. Chavez, 416 U.S. 562, 574-75 (1974).

[270] *Id.*

[271] United States v. Chun, 503 F.2d 533, 542 (9th Cir. 1974).

[272] 503 F.2d 533 (9th Cir. 1974); 12 HOUST. L. REV. 760 (1975).

[273] *Id.* at 542.

[274] *Id.* at 536-37, 542 n.19.

[275] Prejudice could be caused by late notice in a number of ways. First, the defendant might simply not have enough time to analyze the wiretap evidence and make his objections in timely fashion. Second, his memory of the actual events could have dimmed, or he may have destroyed documents or files which would have been helpful in refuting the wiretap evidence. Third, if the defendant feels he has inadequate time to analyze the evidence before trial, he will normally request a postponement of the trial date. If the indictment was initially delayed, and the postponement was due to the government's failure to serve timely

the statutory purpose would not have been adequately fulfilled, and the courts have generally agreed that suppression would be proper.[276] The statutory purpose has probably been satisfied if "the individual has been afforded a reasonable opportunity to prepare an adequate response to the evidence which has been derived from the interception."[277]

In sum, the inventory requirement of Title III is a central or at least functional part of the statutory scheme, and a violation of its provisions may lead to suppression. In the absence of a showing of prejudice, however, late service of the inventory still provides actual notice, satisfies the constitutional and statutory purpose, and renders suppression unnecessary.

C. *No Service*

Complete failure to serve the inventory falls under the same analytical framework as late service. The result is different, however, because failure to serve provides no notice at all and so cannot achieve the statutory or constitutional aim. Suppression must follow, therefore, unless it is clear that the defendants had actual notice from other sources.[278] Actual notice, even from a source other than a formal inventory, satisfies the statutory purpose

notice, the defendant may have a claim that the delay violated his due process or speedy trial rights under the fifth and sixth amendments. *See, e.g.*, United States v. Daneals, 370 F. Supp. 1289 (W.D.N.Y. 1974) (excessive preindictment delay due to inaction or misconduct by the government is prima facie prejudicial); United States v. Wilson, 357 F. Supp. 619 (E.D. Pa. 1972), *appeal dismissed*, 492 F.2d 1345 (3d Cir. 1973), *cert. granted*, 417 U.S. 908 (1974) (delay of 16 months between completion of investigation and indictment unreasonable, despite government's claim that the time was needed to organize the evidence in the case); United States v. Rutkowski, 337 F. Supp. 340 (E.D. Pa. 1971) (delay of nearly five years unreasonable). *But see* United States v. Galardi, 476 F.2d 1072 (9th Cir. 1973), *cert. denied*, 414 U.S. 839 (1974) (delay of more than three years not unreasonable even though defendants asserted dimming of memory and a missing helpful witness); United States v. Pritchard, 458 F.2d 1036 (7th Cir.), *cert. denied*, 407 U.S. 911 (1972) (four and one-half year delay not unreasonable when defendant was only able to allege prejudice in conclusory fashion).

[276] *See, e.g.*, United States v. Lawson, 334 F. Supp. 612, 616-17 (E.D. Pa. 1971).

[277] United States v. Chun, 503 F.2d 533, 538 (9th Cir. 1974).

[278] Although the point has not been specifically litigated, the government should carry the burden of persuasion on the issue of actual notice; since the notice issue arises only through the government's failure to comply with the statute, the prosecution should not be permitted to use its violation to its own benefit.

Since a motion for discovery or for suppression would appear on the record on appeal, the appellate court may frequently be certain that the defendants actually had timely notice. But if the record does not reveal facts sufficient to determine actual notice, the best practice would probably be to remand for a hearing, with the government carrying the burden of proof. For cases in which the defendants clearly had notice from other sources, see United States v. Wolk, 466 F.2d 1143, 1144 (8th Cir. 1972); United States v. Kohne, 358 F. Supp. 1053, 1057 (W.D. Pa.), *aff'd*, 487 F.2d 1395 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974).

and remedies a failure to serve.[279] It seems clear, however, that suppression should result when there is neither actual notice nor service of inventory.[280]

In *Chun*, currently the leading case in this area, no formal inventories were ever served.[281] The Ninth Circuit determined that the defendants were entitled to actual notice, and remanded to the district court to determine "whether the underlying statutory purpose behind the § 2518(8)(d) formal notice provisions has been satisfied in spite of appellees' failure to receive such formal notice."[282] On remand the district court ordered suppression because it found that the defendants did have actual notice, but not within the statutory ninety-day period.[283]

Although the court of appeals opinion is well reasoned, the conclusion of the district court seems plainly wrong. Actual notice is a substitute for and stands on the same basis as formal inventory notice.[284] The purpose of both formal and actual notice is to prevent secret searches and to give the defendant an opportunity to prepare his defense.[285] If the defendant is not prejudiced, delay in service of formal notice should not be grounds for suppression.[286] Actual notice should be governed by the same standard, and

---

[279] In United States v. Wolk, 466 F.2d 1143 (8th Cir. 1972), two defendants were served late and one was never served at all, and the district court ordered suppression of the wiretap evidence. The Eighth Circuit reversed, noting that the record showed that the defendants had ample actual notice. After arraignment, the defendants' counsel were given an opportunity to inspect and copy transcripts as well as the actual tapes. Counsel for each of the defendants thereafter received copies of the application, affidavit, and order of interception, and the defendants were able to make a timely motion to suppress. *Id.* at 1144-45. The court concluded:

> Arguably, then, when a person has actual notice that his conversations have been intercepted, both the statutory and constitutional requirements have been substantially complied with.... We do not believe that the use of formal inventories is an end unto itself. Surely neither the Congress nor the constitution would require such emphasis of form over substance.

Id. at 1145-46.

[280] Title III actually requires the government to give the defendant notice twice. The first time is the inventory required by 18 U.S.C. § 2518(8)(d) (1970). The government must also furnish the defendants, not less than ten days before trial, with copies of the court order and application under which the order was obtained. *Id.* § 2518(9). A total failure ever to give the defendants notice would thus render the evidence inadmissible for violation of both sections. If the defendants do not receive notice until it is too late to prepare an adequate defense, then they may ask for a postponement of the trial, or attempt to prove prejudice and thus obtain suppression. *See* note 275 *supra*.

[281] 503 F.2d at 536.

[282] *Id.* at 542 (*citing* 18 U.S.C. § 2518(8)(d) (1970)).

[283] United States v. Chun, 386 F. Supp. 91, 95 (D. Hawaii 1974).

[284] United States v. Wolk, 466 F.2d 1143, 1145 (8th Cir. 1972).

[285] *See* note 240 and accompanying text *supra*.

[286] *See* notes 255-77 and accompanying text *supra*.

should be sufficient to satisfy the constitutional and statutory requirements if it is sufficiently prompt to permit a reasonable opportunity to prepare an adequate response to the evidence.

The district court in *Chun* specifically found that there was "insufficient evidence to sustain any of the claims of prejudice."[287] As in the delayed service situation, actual notice coupled with lack of prejudice should not result in suppression. The *Chun* court's decision to suppress is therefore incorrect, even though actual notice fell outside the ninety-day limit. The suppression remedy should be reserved for cases in which the defendants either were given no actual notice at all or can show that notice was received so late that their ability to analyze and attack the wiretap evidence was impaired.[288]

D. *Deliberate Failure to Serve*

The problems considered up to this point arose because law enforcement officers inadvertently or mistakenly failed to comply with the statute. In two recent cases, however, the violation of the statute was deliberate. *People v. Hueston*[289] and *United States v. Eastman*[290] originated from the same wiretap, but on identical facts the New York Court of Appeals and the Third Circuit reached opposite conclusions.

The violation arose from the express language of the authorization order, which purported to waive the notice requirement entirely. The defendants received no inventories[291] and moved to suppress in both the state and federal actions on the ground that the language of the order violated the statute and rendered the order void.[292]

---

[287] 386 F. Supp. at 94.

[288] The existence of actual notice is frequently inferred from motions for discovery or motions to suppress. *See* note 278 *supra*. Defense counsel should be aware, therefore, that if he chooses to attack the wiretap evidence by any pretrial motion, he may be giving up any chance to press a claim that he did not receive timely notice. It might appear that the defense counsel could, in the event of a failure to serve an inventory, intentionally make no motions for discovery or suppression to press a claim that he was not given timely notice. This subterfuge is not likely to be popular, however. A motion to suppress on any of several other grounds, such as minimization or amendment, is usually far more likely to succeed than a claim of lack of notice, and the defense counsel would run grave risks of compromising his client's case if he purposely passed up opportunities to inspect the evidence in order to preserve an uncertain, bogus claim.

[289] 34 N.Y.2d 116, 312 N.E.2d 462, 356 N.Y.S.2d 272 (1974), *cert. denied*, 421 U.S. 947 (1975).

[290] 465 F.2d 1057 (3d Cir. 1972).

[291] 34 N.Y.2d at 119-20, 312 N.E.2d at 463, 356 N.Y.S.2d at 275-76; United States v. Eastman, 465 F.2d 1057, 1059 (3d Cir. 1972).

[292] 34 N.Y.2d at 119, 312 N.E.2d at 463, 356 N.Y.S.2d at 275; United States v. Eastman, 465 F.2d 1057, 1059 (3d Cir. 1972).

The *Eastman* court accepted this argument, reasoning that wiretapping is an invasion of privacy that must be conducted in strict conformity with the letter of the law.[293] The Third Circuit affirmed, ruling that:

> The touchstone of our decision on this aspect of the case at bar is not one in which an inventory was delayed but rather is one in which specific provisions of Title III were deliberately and advertently not followed. In other words the failure to file the notice or inventory is no mere ministerial act. It resulted from a judicial act which on its face deliberately flouted and denigrated the provisions of Title III designated for the protection of the public. This we cannot countenance.[294]

The New York Court of Appeals in *Hueston* considered the Third Circuit's opinion but did not agree. The inventory requirement of Title III does not require any particular set of words in the warrant, the court said, but rather guarantees actual notice to the defendants that they have been the subject of electronic surveillance.[295] The waiver of notice in the warrant was of no importance, the court held, because the language was contrary to statute and a nullity, and the only crucial question was whether the defendants actually received notice. "In short, the guarantee we are concerned with here applies to the notice itself, not to the wording of the warrant; and consequently, to suppress the evidence, a defendant must show a failure of notice."[296]

Since the defendants had indisputably moved for discovery of the affidavits, application, and order within ninety days after the termination of surveillance, the court concluded that the defendants had actual notice within the statutory limit despite the failure to serve the inventory, and the purpose of the statutory notice requirement had been fulfilled.[297] The court therefore differed with the Third Circuit and held that the wiretap evidence was properly admissible.[298]

Although the *Hueston* court considered and rejected the Third Circuit's approach, on balance *Eastman* is the sounder view. The New York court treated the intentional waiver case as though it were no different from an unintentional failure to serve notice, and would evidently resolve both on a simple determination of

---

[293] United States v. Eastman, 326 F. Supp. 1038 (M.D. Pa. 1971), *aff'd*, 465 F.2d 1057 (3d Cir. 1972).

[294] 465 F.2d at 1062.

[295] 34 N.Y.2d at 119-20, 312 N.E.2d at 464, 356 N.Y.S.2d at 275.

[296] *Id.*

[297] *Id.* at 120, 312 N.E.2d at 464, 356 N.Y.S.2d at 276.

[298] *Id.* at 123, 312 N.E.2d at 465, 356 N.Y.S.2d at 277-78.

actual notice. There are sound reasons why the two situations should not be treated in the same way, however. One of the original purposes of the suppression rule was to curb government lawlessness by providing some meaningful penalty, as well as to give the defendant a means of vindicating his rights.[299] Justice Brandeis's warning that "[i]f the Government becomes a lawbreaker, it breeds contempt for law"[300] is nowhere more pertinent than to wiretapping and Title III. The potential for intrusion on individual privacy and wholesale violation of constitutional rights is nowhere greater, and the Title III safeguards must be zealously applied.[301] If inadvertent failures to comply with the statute can be cause for suppression,[302] then surely a demonstrated advance intent to ignore the law is an even clearer case, even if the defendants chance to learn of the tap on their own. Judges should not be permitted to waive or ignore clear statutory safeguards simply because later events rendered the judges' actions harmless.

E. *Persons Not Named in Authorization Order*

According to the letter of the statute, the inventory requirement is mandatory only for those persons actually named in the authorization order.[303] The judge may order notice to such other persons as he "may determine in his discretion . . . is in the interest of justice."[304] Until recently this provision has been upheld as constitutional and has generally barred motions for suppression on the lack of notice ground when made by persons not named in the order.[305]

---

[299] *See* Ker v. California, 374 U.S. 23 (1963); Mapp v. Ohio, 367 U.S. 643 (1961); Weeks v. United States, 232 U.S. 383 (1914).

[300] Olmstead v. United States, 277 U.S. 438, 485 (1928) (dissenting opinion, Brandeis, J.).

[301] The tremendous scientific and technological developments that have taken place in the last century have made possible today the widespread use and abuse of electronic surveillance techniques. As a result of these developments, privacy of communication is seriously jeopardized by these techniques of surveillance. . . . No longer is it possible, in short, for each man to retreat into his home and be left alone.

LEGISLATIVE HISTORY 2154.

[302] An inadvertent failure to minimize can be a ground for suppression, for instance, if the monitoring officers do not take affirmative steps to develop a minimization plan. *See* note 110 and accompanying text *supra*.

[303] 18 U.S.C. § 2518(8)(d) (1970).

[304] *Id.*

[305] *Accord*, United States v. Rizzo, 492 F.2d 443, 447 (2d Cir.), *cert. denied*, 417 U.S. 944 (1974); United States v. Cafero, 473 F.2d 489, 498-99 (3d Cir. 1973), *cert. denied*, 417 U.S. 918 (1974). *Contra*, United States v. Whitaker, 343 F. Supp. 358, 368 (E.D. Pa. 1972), *rev'd*, 474 F.2d 1246 (3d Cir.), *cert. denied*, 412 U.S. 953 (1973).

One district court wrote simply:

The Ninth Circuit's opinion in *Chun* for the first time challenged the proposition that only those named in the order must be served, and raised serious doubts about the validity of the discretion provision.[306] Basing its decision on a constitutional guarantee of notice, and reasoning that "the unnamed but overheard are also entitled to Fourth Amendment protection," the court held that the right to notice extends to all those whom the government proposes to indict, even if they are not named in the warrant.[307] On the statutory level, the court ruled that implicit in the grant of discretion to the judge is a requirement that the government furnish the court with accurate and complete information as to whose communications were intercepted and who is to be indicted.[308]

Although the *Chun* opinion is in the minority,[309] it is the most critical evaluation to date of notice to unnamed persons, and its reasoning is persuasive. If there is a constitutional guarantee of notice, it should at a minimum apply to prospective defendants, for the defendant is most in need of time to prepare his case and analyze the evidence against him. In the case of a wiretap, where the tapes may run for hundreds of hours and transcription and analysis may take thousands, it may take months for a defendant to prepare motions to suppress, and prompt notice is thus essential to

---

> As this section reads, the issuing judge, in his discretion, need only serve inventories on those persons named in the order; he is not required to serve inventories on all persons whose calls were intercepted. Defendants have shown nothing to indicate Judge Watkins abused his discretion by serving only the defendants named in the orders.

United States v. Curreri, 363 F. Supp. 430, 435 (D. Md. 1973).

The government may not evade the notice requirement by purposely omitting names from the order. 18 U.S.C. § 2518(4)(a) (1970); United States v. Bernstein, 509 F.2d 996, 1003-04 (4th Cir. 1975).

[306] 503 F.2d at 537.

[307] *Id.* at 536-37.

[308] To discharge this obligation [of exercise of discretion] the judicial officer must have, at a minimum, knowledge of the particular categories into which fall all the individuals whose conversations have been intercepted. Thus, while precise identification of each party to an intercepted communication is not required, a description of the general class, or classes, which they comprise is essential to enable the judge to determine whether additional information is necessary for a proper evaluation of the interests of the various parties. Furthermore, although the judicial officer has the duty to cause the filing of the inventory, it is abundantly clear that the prosecution has greater access to and familiarity with the intercepted communications. Therefore we feel justified in imposing upon the latter the duty to classify all those whose conversations have been intercepted, and to transmit this information to the judge.

Id. at 540 (footnote omitted). *Accord,* United States v. Donovan, 513 F.2d 337, 342-43 (6th Cir. 1975); United States v. Swanson, 399 F. Supp. 441, 444 (D. Nev. 1975).

[309] *See* cases cited in note 305 *supra.*

an effective defense.[310] Although the statute distinguishes between those who are named in the order and those who are not, it is clear that defendants in both classes have equal need of notice. The *Chun* opinion does not declare the discretionary portion of the inventory requirement unconstitutional, but it is difficult to see how that section can stand unless it is read to require the judge to use his discretion to ensure that each prospective defendant has actual notice.[311]

The second branch of the *Chun* opinion is equally persuasive. The statute imposes upon the judge, not the prosecutor, the duty of instituting service of inventories and determining who should be served. The information that the judge needs for his determination is usually within the sole possession of the law enforcement authorities, however, and a requirement that the government fully inform the judge of the changing status of the persons affected by the wiretap seems necessary.[312] If the government withholds information from the judge, notice may not reach those who should receive it, and the statutory purposes would be thwarted.

CONCLUSION

The Constitution and Title III govern the execution of wiretaps and set standards for conduct of government agents during electronic surveillance. Agents should be aware that they must carry out four major post-authorization duties, and that failure in any one of them may result in suppression of part or all of the wiretap evidence. Agents must minimize interception of nonpertinent conversations, amend the eavesdropping order under certain circumstances, seal the tapes upon termination of the tap, and cause service of a statutory notice upon certain individuals. Each of these duties serves to protect the rights of the suspects and of the general public, but each presents legal pitfalls for the careless government agent.

The definition of the statutory term "interception" is a critical

---

[310] *See* note 275 *supra*.

[311] *See* United States v. Donovan, 513 F.2d 337, 342-43 (6th Cir. 1975); United States v. Chun, 503 F.2d 533, 537-38 (9th Cir. 1974). *Chun* held that the notice served on unnamed persons contain "at a minimum" all the information contained in a formal inventory. *Id.* at 537-38. To arrive at this position, the court must have believed that the contents of the formal inventory amount to the constitutional minimum for actual notice. This definition of actual notice should be weighed carefully when other courts determine whether a defendant who did not receive an inventory nevertheless had actual notice.

[312] *See* note 308 *supra*.

threshold question in a discussion of minimization. Although the statute is ambiguous and the cases have dealt poorly with the problem, the only workable definition is that both overhearing and recording constitute an interception. The courts have generally construed the minimization requirement to mean that agents must make a reasonable effort under the circumstances to minimize interception of nonpertinent conversations. Reasonableness is evaluated on a case-by-case basis using the perspective of the agent on the spot, and the courts have generally used up to six major variables to evaluate the agents' practices in each case.

Although Title III provides for a suppression remedy, the statute does not specify how much evidence is to be suppressed when agents fail to minimize. Suppression of all evidence is used rarely, and is reserved for cases of total failure to minimize. When agents attempt to minimize but fail, the courts more often suppress only the improperly intercepted conversations.

When agents intercept evidence of a "new crime," they may be required to obtain an immediate amendment of the eavesdropping order. This duty does not apply to interception of "new persons," and probably does not apply if the tap ends immediately after perception of a new crime. When the tap continues, however, agents should quickly obtain an amendment even though several courts have excused apparent violations of the strict terms of the statute.

The sealing and notice requirements apply after the wiretap is removed, and thus operate as conditions subsequent. The courts have been reluctant to allow violation of these conditions to result in suppression, and most courts will excuse trivial variations from the precise requirements of the statute. Nevertheless, a serious violation, such as failure to seal the tapes or failure to serve notice, may still cause suppression of all the wiretap evidence.

Wiretapping is a powerful tool of law enforcement, but if abused it is an equally powerful invasion of innocent citizens' rights. The officials entrusted with the use of the wiretap must work with a healthy respect for the rights of the suspect as well as the rights of third parties who chance to use the telephone. When the officials err, the courts must be quick to correct the error and enforce the law; too often judges have deferred to the agents' blithe reassurances of good faith, and too often they have balked at applying the statutory remedies. Concluding its discussion of a minimization case, one court of appeals wrote:

> It is clear . . . that a court should not admit evidence derived

from an electronic surveillance order unless . . . it is left with the conviction that on the whole the agents have shown a high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion.[313]

Andrew M. Low

---

[313] United States v. Tortorello, 480 F.2d 764, 784 (2d Cir.), *cert. denied*, 414 U.S. 866 (1973).